Senate Testimony

Heading Toward An EMP Catastrophe*

Ambassador R. James Woolsey
Chairman, Foundation for Defense of Democracies
Former Director of Central Intelligence

Senate Homeland Security and Governmental Affairs Committee

Washington, DC
July 22, 2015

FDD
FOUNDATION FOR DEFENSE OF DEMOCRACIES
1726 M Street NW ● Suite 700 ● Washington, DC 20036

For over a decade now, since the Congressional EMP Commission delivered its first report to Congress eleven years ago in July of 2004, various Senate and House committees have heard from numerous scientific and strategic experts the consensus view that natural and manmade electromagnetic pulse (EMP) is an existential threat to the survival of the American people, that EMP is a clear and present danger, and that something must be done to protect the electric grid and other life sustaining critical infrastructures--immediately.

Yet this counsel and the cost-effective solutions proposed to the looming EMP threat have been ignored. Continued inaction by Washington will make inevitable a natural or manmade EMP catastrophe that, as the Congressional EMP Commission warned, could kill up to 90 percent of the national population through starvation, disease, and societal collapse.

Indeed, some actions taken by the Congress, the White House, and the federal bureaucracy are impeding solutions, making the nation more vulnerable, and helping the arrival of an EMP catastrophe. More about that later.

Why has Washington failed to act against the EMP threat? A big part of the problem is that policymakers and the public still fail to understand that EMP, and the catastrophic consequences of an EMP event, are not science fiction.

The EMP threat is as real as the Sun and as inevitable as a solar flare.

The EMP threat is as real as nuclear threats from Russia, China, North Korea, and Iran. Nuclear EMP attack is part of the military doctrines, plans and exercises of all of these nations for a revolutionary new way of warfare that focuses on attacking electric grids and civilian critical infrastructures--what they call Total Information Warfare or No Contact Wars, and what some western analysts call Cybergeddon or Blackout Wars.

The nuclear EMP threat is as real as North Korea's KSM-3 satellite, that regularly orbits over the U.S. on the optimum trajectory and altitude to evade our National Missile Defenses and, if the KSM-3 were a nuclear warhead, to place an EMP field over all 48 contiguous United States.

The EMP threat is as real as non-nuclear radiofrequency weapons that have already been used by terrorists and criminals in Europe and Asia, and no doubt will sooner or later be used here against America.

A Clear And Present Danger

EMP, while still inadequately understood by policymakers and the general public, has been the subject of numerous major scientific and strategic studies. All of these warn by consensus that a natural or nuclear EMP, in the words of the Congressional EMP Commission, "Is one of a small number of threats that has the potential to hold our society seriously at risk" and "Is capable of causing catastrophe for the nation." Such is

the warning not only of the Congressional EMP Commission, but of studies by the Congressional Strategic Posture Commission, the National Academy of Sciences, the Department of Energy, the National Intelligence Council, a U.S. Federal Energy Regulatory Commission report coordinated with the Department of Defense and Oak Ridge National Laboratory, and numerous other reports.

Yet a recent Wall Street Journal article (May 1, 2015) on NORAD moving back into Cheyenne Mountain and spending $700 million to further harden the mountain against a nuclear EMP attack from North Korea, received hundreds of comments from shocked readers, half of whom still think that EMP is science fiction.

Nuclear EMP. We know that EMP is not science fiction but an existential threat that would have catastrophic consequences for our society because of high-altitude nuclear tests by the U.S. and Russia during the early Cold War, decades of underground nuclear testing, and over 50 years of tests using EMP simulators. For example, in 1961 and 1962, the USSR conducted several EMP tests in Kazakhstan above its own territory, deliberately destroying the electric grid and other critical infrastructures over an area larger than Western Europe. The Congressional EMP Commission based its threat assessment partially on using EMP simulators to test modern electronics--which the Commission found are over one million times more vulnerable than the electronics of the 1960s.

One prominent myth is that a sophisticated, high-yield, thermonuclear weapon is needed to make a nuclear EMP attack. In fact, the Congressional EMP Commission found that virtually any nuclear weapon--even a primitive, low-yield atomic bomb such as terrorists might build--would suffice. The U.S. electric grid and other civilian critical infrastructures--for example, communications, transportation, banking and finance, food and water--have never been hardened to survive EMP. The nation has 18 critical infrastructures--all 17 others depend upon the electric grid.

Another big myth is that a sophisticated long-range missile is needed to deliver an EMP attack. The iconic EMP attack detonates a single warhead about 300 kilometers high over the center of the U.S., generating an EMP field over all 48 contiguous United States.

However, any warhead detonated 30 kilometers high anywhere over the eastern half of the U.S. would collapse the Eastern Grid. The Eastern Grid generates 75 percent of U.S. electricity and supports most of the national population. Such an attack could be made by a short-range Scud missile launched off a freighter, by a jet fighter or small private jet doing a zoom climb, or even by a meteorological balloon.

According to a February 2015 article by President Ronald Reagan's national security brain trust--Dr. William Graham who was Reagan's Science Advisor and ran NASA, Ambassador Henry Cooper who was Director of the Strategic Defense Initiative, and Fritz Ermarth who was Chairman of the National Intelligence Council--North Korea and Iran have both practiced the iconic nuclear EMP attack against the United States. Both nations have orbited satellites on south polar trajectories that evade U.S. early warning

radars and National Missile Defenses. North Korea and Iran have both orbited satellites at altitudes that, if the satellites were nuclear warheads, would place an EMP field over all 48 contiguous United States.

Dr. Graham and his colleagues in their article warn that Iran should already even be regarded as having nuclear weapons and missiles capable of making an EMP attack against the U.S., or against any nation on Earth.

North Korea and Iran have also apparently practiced making a nuclear EMP attack using a short-range missile launched off a freighter. Such an attack could be conducted anonymously to escape U.S. retaliation--thus defeating nuclear deterrence.

Natural EMP. We know that natural EMP from the Sun is real. Coronal mass ejections traveling over one million miles per hour strike the Earth's magnetosphere, generating geomagnetic storms every year. Usually these geo-storms are confined to nations at high northern latitudes and are not powerful enough to have catastrophic consequences. In 1989, the Hydro-Quebec Storm blacked-out half of Canada for a day causing economic losses amounting to billions of dollars.

However, we are most concerned about the rare solar super-storm, like the 1921 Railroad Storm, which happened before American civilization became dependent for survival upon electricity and the electric grid. The National Academy of Sciences estimates that if the Railroad Storm were to recur today, there would be a nationwide blackout with recovery requiring 4-10 years, if recovery is possible at all.

The most powerful geomagnetic storm on record is the 1859 Carrington Event. Estimates are that Carrington was about 10 times more powerful than the 1921 Railroad Storm and 100 times more powerful than the 1989 Hydro-Quebec Storm. The Carrington Event was a worldwide phenomenon, causing forest fires from flaring telegraph lines, burning telegraph stations, and destroying the just laid intercontinental telegraph cable at the bottom of the Atlantic Ocean.

If a solar super-storm like the Carrington Event recurred today, it would collapse electric grids and life-sustaining critical infrastructures worldwide, putting at risk the lives of billions.

NASA in July 2014 reported that two years earlier, on July 23, 2012 , the Earth narrowly escaped another Carrington Event. A Carrington-class coronal mass ejection crossed the path of the Earth, missing our planet by just three days. NASA assesses that the resulting geomagnetic storm would have had catastrophic consequences worldwide.

We are overdue for recurrence of another Carrington Event. The NASA report estimates that likelihood of such a geomagnetic super-storm is 12 percent per decade. This virtually guarantees that Earth will experience a catastrophic geomagnetic super-storm within our lifetimes or that of our children.

Radio-Frequency Weapons (RFWs). Just as nuclear and natural EMP are not science fiction, we also know that the EMP threat from non-nuclear weapons, commonly called Radio-Frequency Weapons, is real. Terrorists, criminals, and even disgruntled individuals have already made localized EMP attacks using RFWs in Europe and Asia. Probably sooner rather than later, the RFW threat will come to America.

RFWs typically are much less powerful than nuclear weapons and much more localized in their effects, usually having a range of one kilometer or less. Reportedly, according to the Wall Street Journal, a study by the U.S. Federal Energy Regulatory Commission warns that a terrorist attack that destroys just 9 key transformer substations could cause a nationwide blackout lasting 18 months.

RFWs offer significant advantages over guns and bombs for attacking the electric grid. The EMP field will cause widespread damage of electronics, so precision targeting is much less necessary. And unlike damage from guns and bombs, an attack by RFWs is much less conspicuous, and may even be misconstrued as an unusual accident arising from faulty components and systemic failure.

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] 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).

All Hazards Strategy. The Congressional EMP Commission recommended an "all hazards" strategy to protect the nation by addressing the worst threat--nuclear EMP attack. Nuclear EMP is worse than natural EMP and the EMP from RFWs because it combines several threats in one. Nuclear EMP has a long-wavelength component like a geomagnetic super-storm, a short-wavelength component like Radio-Frequency Weapons, a mid-wavelength component like lightning--and is potentially more powerful and can do deeper damage than all three.

Thus, protecting the electric grid and other critical infrastructures from nuclear EMP attack will also protect against a Carrington Event and RFWs. Moreover, protecting against nuclear EMP will also protect the grid and other critical infrastructures from the worst over-voltages that may be generated by severe weather, physical sabotage, or cyber-attacks.

EMP--The Ultimate Cyber Weapon

Ignorance of the military doctrines of potential adversaries and a failure of strategic imagination is setting America up for an EMP Pearl Harbor that could easily be avoided--if we would only heed that terrorist sabotage of electric grids and cyber-attacks are early warning indicators. In fact, in the military doctrines, planning, and exercises of Russia, China, North Korea and Iran, nuclear EMP attack is the ultimate weapon in an

all-out cyber operation aimed at defeating nations by blacking-out their electric grids and other critical infrastructures.

For example, Russian General Vladimir Slipchenko in his military textbook *No Contact Wars* describes the combined use of cyber viruses and hacking, physical attacks, non-nuclear EMP weapons, and ultimately nuclear EMP attack against electric grids and critical infrastructures as a new way of warfare that is the greatest Revolution in Military Affairs (RMA) in history. Like Nazi Germany's Blitzkrieg ("Lightning War") Strategy that coordinated airpower, armor, and mobile infantry to achieve strategic and technological surprise that nearly defeated the Allies in World War II, the New Blitzkrieg is, literally and figuratively an electronic "Lightning War" so potentially decisive in its effects that an entire civilization could be overthrown in hours. According to Slipchenko, EMP and the new RMA renders obsolete modern armies, navies and air forces. For the first time in history, small nations or even non-state actors can humble the most advanced nations on Earth.

China's military doctrine sounds an identical theme. According to People's Liberation Army textbook *World War, the Third World War--Total Information Warfare*, written by Shen Weiguang (allegedly the inventor of Information Warfare), "Therefore, China should focus on measures to counter computer viruses, nuclear electromagnetic pulse...and quickly achieve breakthroughs in those technologies...":

With their massive destructiveness, long-range nuclear weapons have combined with highly sophisticated information technology and information warfare under nuclear deterrence....Information war and traditional war have one thing in common, namely that the country which possesses the critical weapons such as atomic bombs will have "first strike" and "second strike retaliation" capabilities....As soon as its computer networks come under attack and are destroyed, the country will slip into a state of paralysis and the lives of its people will ground to a halt. Therefore, China should focus on measures to counter computer viruses, nuclear electromagnetic pulse...and quickly achieve breakthroughs in those technologies in order to equip China without delay with equivalent deterrence that will enable it to stand up to the military powers in the information age and neutralize and check the deterrence of Western powers, including the United States.

Iran in a recently translated military textbook endorses the theories of Russian General Slipchenko and the potentially decisive effects of nuclear EMP attack some 20 times. An Iranian political-military journal, in an article entitled “Electronics To Determine Fate Of Future Wars,” states that the key to defeating the United States is EMP attack and that, “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.":

Advanced information technology equipment exists which has a very high degree of efficiency in warfare. Among these we can refer to communication and information gathering satellites, pilotless planes, and the digital system....Once you confuse the enemy communication network you can also disrupt the work of the enemy command

and decision-making center. Even worse, today when you disable a country's military high command through disruption of communications you will, in effect, disrupt all the affairs of that country….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. (Tehran, *Nashriyeh-e Siasi Nezami*, December 1998 - January 1999)

North Korea appears to have practiced the military doctrines described above against the United States--including by simulating a nuclear EMP attack against the U.S. mainland. Following North Korea's third illegal nuclear test in February 2013, North Korean dictator Kim Jong-Un repeatedly threatened to make nuclear missile strikes against the U.S. and its allies. In what was the worst ever nuclear crisis with North Korea, that lasted months, the U.S. responded by beefing-up National Missile Defenses and flying B-2 bombers in exercises just outside the Demilitarized Zone to deter North Korea. On April 9, 2013, North Korea's KSM-3 satellite orbited over the U.S. from a south polar trajectory, that evades U.S. early warning radars and National Missile Defenses, at the near optimum altitude and location to place an EMP field over all 48 contiguous United States. On April 16, 2013, the KSM-3 again orbited over the Washington, D.C.-New York City corridor where, if the satellite contained a nuclear warhead, it could project the peak EMP field over the U.S. political and economic capitals and collapse the Eastern Grid, which generates 75 percent of U.S. electricity. On the same day, parties unknown used AK-47s to attack the Metcalf transformer substation that services San Francisco, the Silicon Valley, and is an important part of the Western Grid. Blackout of the Western Grid, or of just San Francisco, would impede U.S. power projection capabilities against North Korea. In July 2013, a North Korean freighter transited the Gulf of Mexico with two nuclear capable SA-2 missiles in its hold, mounted on their launchers hidden under bags of sugar, discovered only after the freighter tried to return to North Korea through the Panama Canal. Although the missiles were not nuclear armed, they are designed to carry a 10 kiloton warhead, and could execute the EMP Commission's nightmare scenario of an anonymous EMP attack launched off a freighter. All during this period, the U.S. electric grid and other critical infrastructures experienced various kinds of cyber-attacks, as they do every day and continuously.

North Korea appears to have been so bold as to use the nuclear crisis it deliberately initiated to practice against the United States an all-out cyber warfare operation, including computer bugs and hacking, physical sabotage, and nuclear EMP attack.

Just as Nazi Germany practiced the Blitzkrieg in exercises and during the Spanish Civil War (1936-1939), before surprising the Allies in World War II, so terrorists and state actors appear to be practicing now. For example:

--On October 27, 2013, the Knights Templars, a criminal drug cartel, blacked-out Mexico's Michoacan state and its population of 420,000, so they could terrorize the people and paralyze the police. The Knights, cloaked by the blackout, entered towns and villages and publicly executed leaders opposed to the drug trade.

--On June 9, 2014, Al Qaeda in the Arabian Peninsula used mortars and rockets to destroy transmission towers, plunging into darkness all of Yemen, a country of 16 cities and 24 million people. It is the first time in history that terrorists put an entire nation into blackout, and an important U.S. ally, whose government was shortly afterwards overthrown by terrorists allied to Iran.

--In July 2014, according to press reports, a Russian cyber-bug called Dragonfly infected 1,000 electric power-plants in Western Europe and the United States for purposes unknown, possibly to plant logic bombs in power-plant computers to disrupt operations in the future.

--On January 25, 2015, terrorists blacked-out 80 percent of the electric grid in Pakistan, a nation of 185 million people, and a nuclear weapons state.

--On March 31, 2015, most of Turkey's 75 million people experienced a widespread and disruptive blackout, the NATO ally reportedly victimized by a cyber-attack from Iran.

On June 20, 2015, the New York Times reported that administration officials in a classified briefing to Congress on a cyber-attack from China, that stole sensitive U.S. Government data on millions of federal employees, was information warfare "on a scale we've never seen before from a traditional adversary." Yet this and the other ominous threats described above are already forgotten, or relegated to back page news, as policymakers and the public stumble on, seemingly shell-shocked and uncomprehending, to the latest cyber crisis.

We as a nation are not "connecting the dots" through a profound failure of strategic imagination. Like the Allies before the Blitzkrieg of World War II, we are blind to the unprecedented existential threat that is about to befall our civilization--figuratively and literally, from the sky, like lightning.

Washington Dysfunction

The Congressional EMP Commission recommended a plan to protect the national electric grid from nuclear EMP attack, that would also mitigate all lesser threats--including natural EMP, RFWs, cyber bugs and hacking, physical sabotage, and severe weather--for about $2 billion, which is what the U.S. gives away every year in foreign aid to Pakistan. About $10-20 billion would protect all the critical infrastructures from nuclear EMP attack and other threats.

There are other plans that cost much less, and much more, because there are different technologies and strategies for protecting against EMP, and to different levels of risk. Any or all of these plans are commendable. There is no such thing as being over-prepared for an existential threat.

Unfortunately, none of these plans has been implemented. The U.S. electric grid and other civilian critical infrastructures remain utterly vulnerable to EMP because of

lobbying by the electric utilities in Congress, the federal bureaucracy, and the White House.

Lobbying by the electric power industry and their North American Electric Reliability Corporation (NERC) has, so far, thwarted every bill by the U.S. Congress to protect the grid from EMP. For example, in 2010, the House passed unanimously the GRID Act--which was denied a vote in the Senate, because a single Senator on the Energy and Natural Resources Committee put a hold on the bill. If the GRID Act passed in 2010, the national electric grid would already be protected from EMP, a process the EMP Commission estimated would take about 3-5 years.

The SHIELD Act, another bipartisan bill to protect the electric grid, has been stalled in the House Energy and Commerce Committee for years, due to lobbying by the electric utilities.

Even worse, the U.S. Federal Energy Regulatory Commission, which has a too deferential and too cozy relationship with NERC, has approved a NERC proposed standard for protecting the grid from solar storms that has been condemned by the best scientific experts. Dr. William Radasky and John Kappenman, who both served on the Congressional EMP Commission, and other independent experts have written scientific critiques proving that the NERC standard for natural EMP (also called GMD for Geo-Magnetic Disturbance) is based on "junk science" that grossly underestimates the threat from natural EMP.

For example, Kappenman and Radasky, who 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 natural EMP 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."

Dr. 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 natural EMP 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.

Perhaps most revelatory of U.S. FERC's failures, by approving the NERC GMD Standard that grossly underestimates the natural EMP threat from geo-storms--U.S. FERC abandoned its own much more realistic estimate of the natural EMP threat from geo-storms. 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 is indefensible.

The White House has not helped matters by issuing a draft executive order for protecting the national grid from natural EMP--but that trusts NERC and the electric utilities to set the standards.

Nor has the White House or the U.S. FERC challenged NERC's assertion that it has no responsibility to protect the electric grid from nuclear EMP or Radio-Frequency Weapons.

Nor has the White House or the U.S. FERC done anything to prevent NERC and the utilities from misinforming policymakers and the public about the EMP threat and their lack of preparedness to survive and recover from an EMP catastrophe.

Consequently, policymakers in the States who are alarmed by the lack of progress in Washington on EMP preparedness, find themselves seriously disadvantaged in efforts to protect their State electric grids by the utilities and their well-funded lobbyists who falsely claim Washington and the utilities are making great progress partnering on the EMP problem. So far in 2015, State initiatives to protect their electric grids have been defeated by industry lobbyists in Maine, Colorado, and Texas.

Texas State Senator Bob Hall, a former USAF Colonel and himself an EMP expert, characterizes as "equivalent to treason" the behavior of the electric utilities and their lobbyists:

As a Texas State Senator who tried in the 2015 legislative session to get a bill passed to harden the Texas grid against an EMP attack or nature's GMD, I learned firsthand the strong control the electric power company lobby has on elected officials. We did manage to get a weak bill passed in the Senate but the power companies had it killed in the House. A very deceitful document which was carefully designed to mislead legislators was provided by the power company lobbyist to legislators at a critical moment in the process. The document was not just misleading, it actually contained false statements. The EMP/GMD threat is real and it is not "if" but WHEN it will happen. The responsibility for the catastrophic destruction and wide spread death of

Americans which will occur will be on the hands of the executives of the power companies because they know what needs to be done and are refusing to do it. In my opinion power company executives, by refusing to work with the legislature to protect the electrical grid infrastructure are committing an egregious act that is equivalent to treason. I know and understand what I am saying. As a young US Air Force Captain, with a degree in electrical engineering from The Citadel, I was the project officer who led the Air Force/contractor team which designed, developed and installed the modification to "harden" the Minuteman Strategic missile to protect it from an EMP attack. The American people must demand that the power company executives that are hiding the truth stop deceiving the people and immediately begin protecting our electrical grid so that life as we know it today will not end when the terrorist EMP attack comes.

Ironically, while electric power lobbyists are fighting against EMP protection in Washington, Texas, Maine, Colorado and elsewhere, the Iranian news agency MEHR recently reported that Iran is violating international sanctions and going full bore to protect itself from a nuclear EMP attack:

Iranian researchers...have built an Electromagnetic Pulse (EMP) filter that protects country's vital organizations against cyber-attack. Director of Kosar Information and Communication Technology Institute Saeid Rahimi told MNA correspondent that the EMP (Electromagnetic Pulse) filter is one of the country's boycotted products and until now procuring it required considerable costs and various strategies. "But recently Kosar ICT...has managed to domestically manufacture the EMP filter for the very first time in this country," said Rahimi. Noting that the domestic EMP filter has been approved by security authorities, Rahimi added "the EMP filter protects sensitive devices and organizations against electromagnetic pulse and electromagnetic terrorism." He also said the domestic EMP filter has been implemented in a number of vital centers in Iran. (MEHR News Agency, "Iran Builds EMP Filter for 1st Time" June 13, 2015)

What Is To Be Done?

Congress should pass the Critical Infrastructure Protection Act (CIPA), which requires the Department of Homeland Security to adopt a new National Planning Scenario focused on EMP; to develop plans to protect the critical infrastructures; and for emergency managers and first responders to plan and train to protect and recover the nation from an EMP catastrophe. CIPA will enable DHS to draw upon the deep expertise within the Department of Defense and the Intelligence Community to help protect the critical infrastructures from EMP. Do not let the electric power lobby defeat CIPA or weaken its provisions, as they are presently trying to do.

Reestablish the Congressional EMP Commission. The greatest progress was being made when the EMP Commission existed to advance EMP preparedness. Progress stopped when the EMP Commission terminated in 2008. Currently, the struggle to advance national EMP preparedness is being carried on by a handful of patriotic individuals and Non-Government Organizations who have no official standing

and extremely limited resources. Bring back the EMP Commission with its deep expertise to advise Congress, government at all levels, and the private sector on how best to protect the nation, and to serve as a watchdog and leader for national EMP preparedness.

Pass the SHIELD Act or the GRID Act to establish adequate regulatory authority within the U.S. Government to achieve timely protection of the electric grid--and watch U.S. FERC like a hawk to make sure that regulatory authority is exercised.

Include in the National Defense Authorization Act the simple two-sentence provision below, that could rapidly reverse the trend of America's increasing vulnerability to EMP, by directing the Secretary of Defense to help State governments and the electric utilities protect themselves from an EMP catastrophe:

Energy Security For Military Bases And Critical Defense Industries
Whereas 99 percent of the electricity used by CONUS military bases is supplied by the national electric grid; whereas the Department of Defense has testified to Congress that DoD cannot project power overseas or perform its homeland security mission without electric power from the national grid; whereas the Congressional EMP Commission warned that up to 9 of 10 Americans could die from starvation and societal collapse from a nationwide blackout lasting one year; therefore the Secretary of Defense is directed to urge governors, state legislators, public utility commissions of the 50 states, the North American Electric Reliability Corporation (NERC) and the utilities that supply electricity to CONUS military bases and critical defense industries, to protect the electric grid from a high-altitude nuclear electromagnetic pulse (EMP) attack, from natural EMP generated by a solar super-storm and from other EMP threats including radiofrequency weapons, and to help the states, NERC, public utilities commissions, and electric utilities by providing DoD expertise on EMP and other such support and resources as may be necessary to protect the national electric grid from natural and manmade EMP threats. The Secretary of Defense is authorized to spend up to $2 billion in FY2017 to help protect the national electric grid from EMP.

Ambassador R. James Woolsey is former Director of Central Intelligence and is Chairman of the Foundation for Defense of Democracies.

*I am highly indebted to my friend and colleague, Dr. Peter Vincent Pry, who served on the Congressional EMP Commission and is Executive Director of the EMP Task Force on National and Homeland Security, for assistance in drafting this testimony.