AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 109–30

TERRORISM AND THE EMP THREAT TO HOMELAND SECURITY

HEARING

BEFORE THE

SUBCOMMITTEE ON TERRORISM, TECHNOLOGY AND HOMELAND SECURITY

OF THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

MARCH 8, 2005

Serial No. J–109–5

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

21–324 PDF WASHINGTON : 2005

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

ARLEN SPECTER, Pennsylvania, *Chairman*

ORRIN G. HATCH, Utah
CHARLES E. GRASSLEY, Iowa
JON KYL, Arizona
MIKE DEWINE, Ohio
JEFF SESSIONS, Alabama
LINDSEY O. GRAHAM, South Carolina
JOHN CORNYN, Texas
SAM BROWNBACK, Kansas
TOM COBURN, Oklahoma

PATRICK J. LEAHY, Vermont
EDWARD M. KENNEDY, Massachusetts
JOSEPH R. BIDEN, JR., Delaware
HERBERT KOHL, Wisconsin
DIANNE FEINSTEIN, California
RUSSELL D. FEINGOLD, Wisconsin
CHARLES E. SCHUMER, New York
RICHARD J. DURBIN, Illinois

DAVID BROG, *Staff Director*
MICHAEL O'NEILL, *Chief Counsel*
BRUCE A. COHEN, *Democratic Chief Counsel and Staff Director*

SUBCOMMITTEE ON TERRORISM, TECHNOLOGY AND HOMELAND SECURITY

JON KYL, Arizona, *Chairman*

ORRIN G. HATCH, Utah
CHARLES E. GRASSLEY, Iowa
JOHN CORNYN, Texas
MIKE DEWINE, Ohio
JEFF SESSIONS, Alabama
LINDSEY O. GRAHAM, South Carolina

DIANNE FEINSTEIN, California
EDWARD M. KENNEDY, Massachusetts
JOSEPH R. BIDEN, JR., Delaware
HERBERT KOHL, Wisconsin
RUSSELL D. FEINGOLD, Wisconsin
RICHARD J. DURBIN, Illinois

STEPHEN HIGGINS, *Majority Chief Counsel*
STEVEN CASH, *Democratic Chief Counsel*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

	Page
Kyl, Hon. Jon, a U.S. Senator from the State of Arizona	1
prepared statement	43

WITNESSES

Fonash, Peter, National Communications System Deputy Manger (Acting), Department of Homeland Security, Washington, D.C.	3
Pry, Peter, Senior Staff, Congressional EMP Commission, Washington, D.C.	5
Wood, Lowell, Commissioner, Congressional EMP Commission, Livermore, California	10

SUBMISSIONS FOR THE RECORD

Fonash, Peter, Deputy Manager (Acting), National Communications System, Department of Homeland Security, Washington, D.C., prepared statement	32
Pry, Peter, Senior Staff, Congressional EMP Commission, Washington, D.C., prepared statement	46
Wood, Lowell, Commissioner, Congressional EMP Commission, Livermore, California, prepared statement	51

TERRORISM AND THE EMP THREAT TO HOMELAND SECURITY

TUESDAY, MARCH 8, 2005

UNITED STATES SENATE,
SUBCOMMITTEE ON TERRORISM, TECHNOLOGY
AND HOMELAND SECURITY
COMMITTEE ON THE JUDICIARY
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:35 p.m., in Room SD–226, Dirksen Senate Office Building, Hon. Jon Kyl, Chairman of the Subcommittee, presiding.

Present: Senator Kyl.

OPENING STATEMENT OF HON. JON KYL, A U.S. SENATOR FROM THE STATE OF ARIZONA

Chairman KYL. This hearing of the Subcommittee on Terrorism, Technology, and Homeland Security of the Senate Judiciary Committee will come to order.

Our hearing today is on "Terrorism and the EMP Threat to Homeland Security." Let me indicate that conflicts of interest keep some of my colleagues from being here right now, though several indicated that they were going to try to stop by. The record of the hearing, of course, will be very important. Unfortunately, a conference of Republicans was called, there is a vote going on right now, and some of my Democratic colleagues had some conflicts. But hopefully, we will have some other members join us here before too long.

The subject, as I said, is the electromagnetic pulse and its potential impact as a tool of terrorism against the United States. An attack using EMP, which is a phenomenon created by the detonation of a nuclear weapon, could be devastating to this country and the public and Congress need to pay more attention to that danger. That is the reason for the hearing here today.

Earlier this year, CIA Director Porter Goss gave chilling testimony about missing nuclear material from storage sites in Russia that may have found its way into terrorists' hands. FBI Director Mueller confirmed new intelligence that suggests that al Qaeda is trying to acquire and use weapons of mass destruction in some form against us. And the 9/11 Commission report stated that our biggest failure was one of imagination. No one imagined the terrorists would do what they did on September 11.

I want to explore new and imaginative possibilities of terrorist attacks and methods, and that is why we are here today, to exam-

ine a possibility that poses a grave threat and a crippling impact to our way of life.

Last year, the EMP Commission found that EMP was one of a small number of threats that could hold our society at risk of catastrophic consequences. The effects of an EMP could potentially shock, damage, or even destroy electrical systems that fall within the striking range of a nuclear detonation. And because the United States is heavily dependent on electrical systems to provide all basic services, an EMP attack has the potential to have a cascading effect on all aspects of American society. And finally, particularly because they lack ICBM capability, terrorists could nevertheless use lesser technology to launch an EMP weapon over the United States.

The Commission's report found that our infrastructure, such as electrical power, telecommunications, energy, financial systems, transportation, emergency services, water purification and delivery, food refrigeration, all of these things and more were vulnerable to EMP attack. And in the event of such an attack, those infrastructures would be rendered unusable, thus inflicting widespread disruption or failure on a national scale. The death toll from such an attack is almost unthinkable.

Unfortunately, the House Armed Services Committee hearing on the Commission report occurred on the date of the release of the 9/11 Commission report. As a result, the hearing and the EMP report received virtually no coverage. Thus, we thought it was appropriate to reinitiate that discussion with our hearing here today. We want to review the findings of the Commission, understand the current risk we face, as well as the steps we may need to take and are taking to prepare for such an attack.

We have three very distinguished witnesses with us here today. Dr. Lowell Wood, Jr., is a member of that Commission, a Commissioner on the National Commission to Assess the EMP Threat to the United States. He is a member of the Technical Advisory Group of the U.S. Senate Select Committee on Intelligence, a member of the Undersea Warfare Experts Group of the U.S. House of Representatives Committee on Armed Services, a member of the U.S. Nuclear Strategy Forum, a Visiting Fellow at the Hoover Institution at Stanford University, and an officer and member of the Board of Directors of the Fannie and John Hertz Foundation.

He is also a member of the Laboratory Directors Technical Staff, University of California, Lawrence Livermore National Laboratory, where he has held numerous positions since 1972. He has received numerous awards and prizes for his work and is the author of several hundred publications.

When I introduce Dr. Wood, I will also ask you please to introduce other members of the Commission, who I understand are with us here today, as well.

Dr. Peter Vincent Pry was one of the CIA's chief experts on Soviet plans for EMP attack. During the Cold War, he developed much of what the U.S. Government knows about Soviet planning for nuclear war, and in the post-Cold War period, his work has been central to the U.S. Government's understanding of evolving Russian threat perceptions and military doctrine.

He is the Director of the United States Nuclear Strategy Forum, a nonprofit foundation established to advise Congress on the future threat environment and on the role of nuclear weapons in U.S. national security policy, and recent served on the EMP Commission staff, where he was the chief analyst on foreign views of EMP attack. Dr. Pry holds two Ph.D.s, one in history, the other in international relations. He, too, has authored several books on national security and military issues.

And finally, Dr. Peter Fonash from the Department of Homeland Security, National Communications Acting Deputy Manager. He has been a member of the Senior Executive Service since 1998, has served in both technical and policy positions in the Federal Government. He earned three degrees from the University of Pennsylvania, a B.S. in electrical engineering, an M.S. and Master's of Business Administration at the Wharton School. He also holds a Doctor of Philosophy degree from George Mason University's School of Information Technology and Engineering. His 24 years in Federal service were preceded by 4 years in private industry.

We have a very distinguished panel, as you can see, with us here today. I would also like to recognize the other members of the EMP Commission who are with us here, and as I said, when I introduce Dr. Wood, I would like to ask those of you who are here to stand and be recognized. Their contribution to help us better understand the EMP threat is significant.

I also want to thank Senator Feinstein, who cannot be with us today, for her work, along with her staff, and for her continuing contributions to the work of this Subcommittee.

We hope that even though there are several conflicts that prevent colleagues from being here, there isn't such big news that finally we can't at least get some understanding of this potential threat out to the public so that we can better understand those kinds of threats that we may face in the future.

Let me begin our testimony with Dr. Peter Fonash, and then we will go to Dr. Peter Pry, and then to Dr. Lowell Wood. Dr. Fonash, the floor is yours, and your statements will be put in the record in full. Feel free to quote from them or deviate from them however you wish.

STATEMENT OF PETER M. FONASH, ACTING DEPUTY MANAGER, NATIONAL COMMUNICATIONS SYSTEM, U.S. DEPARTMENT OF HOMELAND SECURITY, WASHINGTON, D.C.

Mr. FONASH. Mr. Chairman, thank you very much. My name is Peter Fonash. I am the Acting Deputy Manager of the National Communications System, NCS. I am honored to appear before you today to discuss the issues surrounding the vulnerabilities of our Nation's critical telecommunications infrastructure to EMP.

The NCS, as you know, is an interagency body that brings together the telecommunications assets of the Federal Government that are of significance to national security and emergency preparedness, NS/EP. The NCS is responsible to ensure the existence of a national telecommunications structure that is responsive to the NS/EP needs of the Federal Government and is capable of providing survivable NS/EP telecommunications services in all circumstances, including conditions of crisis or emergency.

Since the height of the Cold War, the development and maintenance of survivable national telecommunications has been an enduring national objective. To help achieve this objective, President Kennedy in 1963 established the NCS to provide necessary communications for the Federal Government under all conditions, ranging from a normal situation to national emergencies and international crises, including nuclear attack.

When put in place at the height of the Cold War the larger NS/EP goal was promotion of a survivable and resilient national telecommunications infrastructure. The primary focus was on state-based largely monolithic threat. The NS/EP telecommunications role was to enable the U.S. Government to organize national response efforts to those threats.

In the post-9/11 environment, however, the U.S. faces more asymmetric threats and potential targets expanded to include civilian, economic, and other critical targets. This change, fundamental in terms of actors, intent, capability, and tactics, creates new challenges for the U.S. Government.

Regarding EMP, Part 205 of Title 47, Chapter 2, of the Code of Federal Regulations establishes the NCS as the focal point within the Federal Government for all EMP technical data and studies concerning telecommunications. That is a function we have carried out for the last 20 years.

Emerging from the tactical and strategic concerns of the Cold War, analyses of potential resources of electromagnetic disruption of telecommunications services have historically focused most sharply on the effects produced by a nuclear EMP. Yet while nuclear EMP remains the only mechanism to affect widespread electromagnetic disruption to telecommunications, it is important to recognize that the advance of technology has yielded many more tools capable of producing singular telecommunications electromagnetic disruptive effects, known as TEDE, on a more limited but nevertheless significant scale. Such tools are, as a general matter, often less costly than are those necessary to create an EMP. Accordingly, consonant with its EMP telecommunications mission, NCS has expanded its analytic activities to include the full range of TEDE sources, including but not limited to EMP.

With respect to EMP specifically, the NCS has, over the past two decades, conducted numerous studies, simulations, and tests of various elements of the telecommunications infrastructure to electromagnetic interference. The information derived from these tests was used by the equipment manufacturers to implement vulnerability mitigation changes in the design of the switching systems. The results of these tests led to the conclusion that our Nation's telecommunications network will experience serious disruption from EMP, but will be rapidly restored. NCS priority communications programs will provide critical communication capabilities during the restoration period.

Finally, as a part of the interim National Infrastructure Protection Plan, NIPP, recently released by DHS, the NCS serves as the sector-specific agency for the telecommunications sector. The NCS is responsible for assessing and mitigating vulnerabilities to the national telecommunications infrastructure. Accordingly, recognizing communication's pivotal role in deterring and/or recovering

from an attack, the NCS has developed a vulnerability mitigation approach that is designed to address the entire spectrum of potential disruptions to the nation's telecommunications and ensure critical communications will be possible under all conditions. The NCS does not look at EMP or other sources of TEDE in a vacuum, but rather in a larger context of the full range of potential threats to the telecommunications infrastructure.

In summary, the existence of EMP effects has been known since the 1940's. We have tested thoroughly our current generation of core telecommunications switches and have determined that there is minimal lasting EMP effect on these switches. Furthermore, most of our core communications assets are in large, very well constructed facilities which provide a measure of shielding. This situation will evolve as we move to Next Generation Networks, NGN, but we are monitoring this network evolution by testing critical components of the NGN and leveraging DOD testing. Furthermore, the NCS has programs and activities that are designed to minimize the impact of the entire spectrum of potential disruptions, including EMP.

In moving forward, the NCS has a proven history of preparing for and responding to all types of threats. We have demonstrated an ability to develop effective tools and programs combined with a trusted working relationship with industry to continually improve the hardness and survivability of our Nation's communications network.

This concludes my prepared statement. I would be happy to answer questions you may have at this time or any future time.

Chairman KYL. We will take all the testimony and then we will come back and do questions at that time.

[The prepared statement of Mr. Fonash appears as a submission for the record.]

Chairman KYL. Dr. Pry?

STATEMENT OF PETER VINCENT PRY, SENIOR STAFF, CONGRESSIONAL EMP COMMISSION, WASHINGTON, D.C.

Mr. PRY. The EMP Commission sponsored a worldwide survey of foreign scientific and military literature to evaluate the knowledge and possibly of the intentions of foreign states with respect to electromagnetic pulse attack. The survey found that the physics of EMP phenomena and the military potential of EMP attack are widely understood in the international community, as reflected in unofficial and official writings and statements.

The survey of open sources over the past decade finds that knowledge about EMP and EMP attack is evidenced in at least Britain, France, Germany, Israel, Egypt, Taiwan, Sweden, Cuba, India, Pakistan, Iraq under Saddam Hussein, Iran, North Korea, China, and Russia. Numerous foreign governments have invested in hardening programs to provide some protection against nuclear EMP attack, indicating that this threat has broad international credibility.

At least some of the new nuclear weapons states, notably India, are concerned that their military command, control, and communications may be vulnerable to EMP attack. For example, an Indian article citing the views of senior officers in the defense min-

istry concludes, I quote—Mike, if you could put up the first quotation—"The most complicated, costly, controversially and critically important elements of nuclear weaponization are the C3I systems. Saving on a C3I system could be suicidal. With a no first use policy, the Indian communication systems have to be hardened to withstand the electromagnetic pulses generated by an adversarial nuclear first strike. Otherwise, no one will be fooled by the Indian nuclear deterrent."

Many foreign analysts perceive nuclear EMP attack as falling within the category of electronic warfare or information warfare, not nuclear warfare. Indeed, the military doctrines of at least China and Russia appear to define information warfare as embracing a spectrum ranging from computer viruses to nuclear EMP attack.

For example, consider the following quote from one of China's most senior military theorists, Su Tzu-Yun, who is credited by the PRC with inventing information warfare, appearing in his book, World War, The Third World War—Total Information Warfare, and I quote—thank you, Mike, second—"With their massive destructive, long-range nuclear weapons have combined with highly sophisticated information technology and computer technology today and warfare of the looming 21st century. 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 deterrents 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," end quote.

Some foreign analysts, judging from open source statements and writings, appear to regard EMP attack as a legitimate use of nuclear weapons because EMP would inflict no or few prompt civilian casualties. EMP attack appears to be a unique exception to the general stigma attached to nuclear employment by most of the international community in public statements. Significantly, even some analysts in Japan and Germany, nations that historically have been most condemnatory of nuclear and other weapons of mass destruction, in official and unofficial forums, appear to regard EMP attack as morally defensible.

For example, a June 2000 Japanese article in a scholarly journal, citing senior political and military officials, appear to regard EMP attack as a legitimate use of nuclear weapons. The quote is above. Quote, "Although there was little chance that the Beijing authorities would launch a nuclear attack which would incur the disapproval of the international community and which would result in such enormous destruction that it would impede post-war cleanup and policies, a serious assault starting with the use of nuclear weapons which would not harm humans, animals, or property, would be valid. If a nuclear weapon was detonated 40 kilometers

above Taiwan, electromagnetic wave would be propagated which would harm unprotected computers, radar, and IC circuits on the ground within a 100-kilometer radius, and the weapons and equipment which depend on communications electronics technology, whose superiority Taiwan takes pride in, would be rendered combat ineffective at one stroke. If they were detonated in the sky in the vicinity of Ilan, the effects would also extend to the waters near Yanakuni, so it would be necessary for Japan, too, to take care. Those in Taiwan, having lost their advanced technology capabilities, would end up fighting with tactics and technology going back to the 19th century. They would inevitably be at a disadvantage with the PLA and its overwhelming military force superiority."

An article by a member of India's Institute of Defense Studies Analysis openly advocates that India be prepared to make a preemptive EMP attack, both for reasons of military necessity and on humanitarian grounds. This is the next quote. Quote, "A study conducted in the U.S. during the late 1980's reported that a high-yield device exploded about 500 kilometers above the ground can generate an electromagnetic pulse of the order of 50,000 volts over a radius of 2,500 kilometers around the point of burst, which would be collected by any exposed conductor. Such an attack will not cause any blast or thermal effects on the ground below, but it can produce a massive breakdown in the communication system that is certain that most of the land communication networks and military command and control links will be affected and it will undermine our capability to retaliate. This, in fact, is the most powerful incentive for preemptive attack, and a high-altitude exo-atmospheric explosion may not even kill a bird on the ground."

Although India, Pakistan, and Israel are not rogue states, they all presently have missiles and nuclear weapons, giving them the capability to make EMP attacks against their regional adversaries. An EMP attack by any of these states, even if targeted at a regional adversary and not the United States, could collaterally damage U.S. forces in the region and would pose an especially grave threat to U.S. satellites.

Many foreign analysts, particularly in Iran, North Korea, China, and Russia, view the United States as a potential aggressor that would be willing to use its entire panoply of weapons, including nuclear weapons, in a first strike. They perceive the United States as having contingency plans to make a nuclear EMP attack and as being willing to execute those plans under a broad range of circumstances.

Russian and Chinese military scientists in open source writings describe the basic principles of nuclear weapons designed specifically to generate an enhanced EMP effect that they term super-EMP weapons. Super-EMP weapons, according to these foreign open source writings, can destroy even the best protected U.S. military and civilian electronic systems.

Chinese military writings are replete with references to the dependency of United States military forces and civilian infrastructure upon sophisticated electronic systems and to the potential vulnerability of those systems. For example, consider this quote from an official newspaper of the PLA, already up there. Quote, "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, 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."

Russian military writings are also replete with references to the dependency of United States military forces and civilian infrastructure upon sophisticated electronic systems and to the potential vulnerability of those systems. Indeed, Russia made a thinly-veiled EMP threat against the United States on May 2, 1999. During the spring of 1999, tensions between the United States and Russia rose sharply over Operation Allied Force, the NATO bombing campaign against Yugoslavia. A bipartisan delegation from the House Armed Services Committee of the U.S. Congress met in Vienna with their Russian counterparts and the Duma International Affairs Committee, headed by Chairman Vladimir Lukin. The object of the meeting was to reduce U.S.–Russia tensions and seek Russian help in resolving the Balkans crisis. During the meeting, Chairman Lukin and Deputy Chairman Alexander Shaponov chastised the United States for military aggression in the Balkans and warned that Russia was not helpless to oppose Operation Allied Force.

The next quote is there. Quote, "Hypothetically, if Russia really wanted to hurt the United States in retaliation for NATO's bombing of Yugoslavia, Russia could fire a submarine-launched ballistic missile and detonate a single nuclear warhead at high altitude over the United States. The resulting electromagnetic pulse would massively disrupt U.S. communications and computer systems, shutting down everything." Note that quote is from 1999. That is the last semi-official nuclear threat made to the United States by anyone.

Iran, though not yet a nuclear weapons state, has produced some analysis weighing the use of nuclear weapons to destroy cities, compared to information warfare, that includes electromagnetic pulse for the destruction of unprotected circuits. An Iranian analyst describes terrorist information warfare as involving not just computer viruses, but attacks against using electromagnetic pulse.

An Iranian political-military journal in an article entitled, "Electronics To Determine Fate of Future Wars," suggests that the key to defeating the United States is EMP attack. Quote, "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," end quote.

Iranian flight tests of their Shahab-3 medium-range missile that can reach Israel and U.S. forces in the Persian Gulf have in recent years involved several explosions at high altitude, reportedly triggered by a self-destruct mechanism on the missile. The Western press has described these flight tests as failures because the missiles did not complete their ballistic trajectories. Iran has officially described all of these same tests as successful. The flight tests would be successful if Iran were practicing the execution of an EMP attack.

Iran, as noted earlier, has also successfully tested firing a missile from a vessel in the Caspian Sea. A nuclear missile concealed in the hold of a freighter would give Iran, or terrorists, the capability to perform an EMP attack against the United States homeland without developing an ICBM, and with some prospect of remaining anonymous. Iran's Shahab-3 medium-range missile, mentioned earlier, is a mobile missile and small enough to be transported in the hold of a freighter. We cannot rule out that Iran, the world's leading sponsor of international terrorism, might provide terrorists with the means to execute an EMP attack against the United States.

In closing, a few observations about the potential EMP threat from North Korea. North Korean academic writings subscribe to the view voiced in Chinese, Russian, and Iranian writings that computers and advanced communications have inaugurated an information age during which the greatest strength and greatest vulnerability of societies will be their electronic infrastructures. According to North Korean press, Chairman Kim Chong-Il is himself supposedly an avid proponent of this view.

The highest ranking official ever to defect from North Korea, Hwang Chang-Yop, claimed in 1998 that North Korea has nuclear weapons and explained his defection as an attempt to prevent nuclear war. According to Hwang, in the event of war, North Korea would use nuclear weapons, quote, "to devastate Japan to prevent the United States from participating in the defense of South Korea. Would it, the United States, still participate even after Japan is devastated? That is how they think."

Although Hwang did not mention EMP, it is interesting that he described North Korean thinking about nuclear weapons employment as having strategic purposes, nuclear use against Japan, and not tactical purposes, nuclear employment on the battlefield in South Korea. It is also interesting that, according to Hwang, North Korea thinks it can somehow devastate Japan with its tiny nuclear inventory, although how precisely this is to be accomplished with one or two nuclear weapons is unknown.

Perhaps most importantly, note that the alleged purpose of a North Korean nuclear strike on Japan would be to deter the United

States. At the time of Hwang's defection in 1998, North Korea's longest-range missile then operational, the No Dong, limited North Korea's strategic reach to a strike on Japan. Today, North Korea is reportedly on the verge of achieving an ICBM capability with its Taepo Dong-2 missile, estimated to be capable of delivering a nuclear weapon to the United States.

In 2004, the EMP Commission met with very senior Russian military officers who are experts on EMP weapons. They warned that Russian scientists had been recruited by Pyongyang to work on the North Korean nuclear weapons program. They further warned that the knowledge and technology to develop super-EMP weapons had been transformed to North Korea and that North Korea could probably develop these weapons in the near future, within a few years. The Russian officer said that the threat to global security that would be posed by a North Korea armed with super-EMP weapons is unacceptable.

The senior Russian military officers, who claimed to be expressing their personal views to the EMP Commission, said that while the Kremlin could not publicly endorse U.S. preemptive action, Moscow would privately understand the strategic necessity of a preemptive strike by the United States against North Korea's nuclear complex in order to prevent North Korea from achieving a super-EMP weapon that would threaten global civilization.

This concludes my statement. Thank you for the opportunity to share this information with the U.S. Senate.

Chairman KYL. Thank you, Dr. Pry.

[The prepared statement of Mr. Pry appears as a submission for the record.]

Chairman KYL. Dr. Wood, would you please begin by introducing anyone who is here representing the Commission besides yourself?

STATEMENT OF LOWELL WOOD, COMMISSIONER, CONGRESSIONAL EMP COMMISSION, LIVERMORE, CALIFORNIA

Mr. WOOD. Thank you very much, Mr. Chairman. Ladies and gentlemen, my fellow Commissioners and I thank you for the opportunity to testify today on the findings and recommendations of the Commission to Assess the Threat to the United States From Electromagnetic Pulse Attack created by the Congress in Title 14 of Public Law 106–398.

I am here acting today for Dr. William Graham, the Chairman of the Commission, who is prevented from being present today and asked me to convey his regrets and respects to the Committee. I am accompanied by three of my colleague Commissioners, who I would like to introduce very briefly, Dr. Henry Kluepfel, Commissioner of the EMP Commission, Dr. Gordon Soper, EMP Commissioner, and the senior member of the EMP Commission, Dr. John S. Foster, Jr., whose service in the technology components of the national defense dates back to the beginning of World War II.

Chairman KYL. And Dr. Foster probably has testified more times before Congress than I have attended hearings, I might add.

Mr. WOOD. Dr. Foster was doing very notable things for the technological components of the national defense the year that I was born, sir.

Chairman KYL. That doesn't make him old. It is just that he started at a very young age.

[Laughter.]

Mr. WOOD. And gave very distinguished service throughout the over 60 years that he has been so devoted to the national welfare, sir.

At the direction of the Congress, the EMP Commission worked for 2 years in the discharge of its statutory mandate. These efforts have included conducting actual experiments to test the potential vulnerability of modern electronic systems to EMP, and were informed by a global survey of foreign scientific and foreign military literatures to assess the knowledge and, if possible, the intentions of rogue states and other nations with respect to EMP attack, which Dr. Pry, who led this effort for the Commission, just very aptly summarized for the Committee.

The Commission enjoyed access to all information in the possession of the government in the course of its work and was supported by top-quality studies and analyses on the part of many cognizant government and contractor organizations, as indeed was specified in the mandating legislation.

The bottom line is that several classes of potential adversaries, including terrorist groupings, have or can acquire the capability to attack the United States with a high-altitude nuclear weapon generated electromagnetic pulse. A determined adversary can achieve an EMP attack capability without having a high level of either military or nuclear sophisticated. For example, a Scud missile launched from a freighter off the Atlantic coast of the United States could constitute a platform that would enable a terrorist group to mount an EMP attack against roughly half of the United States in population terms. Scud missiles can be purchased inexpensively—they are of the order of $100,000—by anyone, including private collectors in the world's arms markets.

Terrorists might buy, steal, or be given a "no fingerprints" nuclear weapon. For example, North Korea has demonstrated a willingness to sell both missiles and nuclear materials remarkably promiscuously. Iran, the world's leading sponsor of international terrorism, is widely reported to have a nuclear weapons program that is more advanced than previously suspected and is known to have successfully test launched a Scud missile from a vehicle in the Caspian Sea, as Dr. Pry noted, a launch mode that could be adapted, as indeed Secretary of Defense Don Rumsfeld has noted twice in public, could be adapted to support attack against the United States from the sea, including EMP attacks.

A nuclear weapon detonated at altitudes above a few dozen kilometers above the earth's surface would generate a set of electromagnetic pulses of different types as its various outputs interact with the earth's atmosphere and the earth's magnetic field. These electromagnetic pulses propagate from the burst-point of the nuclear weapon to the line of sight on the earth's horizon, potentially covering a vast geographic region and doing so simultaneously, moreover, at the speed of light.

For example, a nuclear weapon detonated at an altitude of 400 kilometers over the central United States would cover with its primary electromagnetic pulse the entire continental United States

and parts of Canada and Mexico. This is indicated on the view graph there, which a detonation at about 500 kilometers over Omaha blankets the entire United States and adjacent portions of Canada and Mexico with high-intensity EMP.

Of course, regional EMP attacks can be comparably devastating to smaller portions of the country and that is indicated for one particular region, the American Southwest, on the view graph here, which a very low altitude burst, at only 75 kilometers and very modest yield, could nonetheless destroy a portion of the United States accounting for almost a third of the gross demographic product.

The immediate effects of EMP are disruption of and damage to electrical and electronic systems and infrastructures. EMP is not reported in the scientific literature to have direct effects on people.

EMP and its effects were observed extensively during the U.S. and Soviet atmospheric test programs in 1962. During the United States' STARFISH nuclear detonation, which was not designed or intended as a generator of EMP, which occurred at an altitude of about 400 kilometers above Johnston Island in the Pacific Ocean, some electrical systems in the Hawaii Islands, 1,400 kilometers distant, were affected. This comparatively weak and distant, and indeed inadvertent, EMP caused the failure of street lighting systems, tripping of circuit breakers, triggering of burglar alarms, and damage to a telecommunications relay system, among other reported and reasonably well-documented effects.

The Russians in their testing that year executed a series of high-altitude nuclear detonations above their test site in South Central Asia on Soviet territory. They report that they observed damage to both overhead and underground buried cables, some at distances of 600 kilometers from under the burst-point. They also observed surge arrestor burnout, spark-gap breakdown, blown fuses, and failures of power supplies of various types, both civilian and military.

What is particularly significant about EMP is that a single high-altitude nuclear detonation can produce EMP effects that can potentially disrupt or damage electronic and electrical systems over much of the United States virtually simultaneously at a time determined by an adversary. Thus, the Commission found that EMP is one of a small number of threat types that has the potential to hold American society seriously at risk and that might also result in the defeat of our military forces.

The electromagnetic field pulses produced by weapons designed and deployed with the intent to produce EMP have a high likelihood of damaging electrical power systems, electronics, and information systems upon which any reasonably advanced society, most specifically including our own, depend vitally. Their effects on systems and infrastructures dependent on electricity and electronics could be sufficiently ruinous as to qualify as catastrophic to the American nation.

Depending on the specific characteristics of the EMP attack, unprecedented cascading failures of our major infrastructures could result, in which failure of one infrastructure could pull down others dependent upon its functioning, and the failure of these, in turn, could seriously impede recovery of the first infrastructure to fail.

In such events, a regional or national recovery would be long and difficult and would seriously degrade the overall viability of the American nation and the safety and even the lives of very large numbers of U.S. citizens.

The primary avenues for EMP imposition of catastrophic damage to the nation are through our electric power infrastructure and thence into our telecommunications, energy, and other key infrastructures. These, in turn, can seriously impact other vital aspects of our Nation's life, including the financial system, means of getting food, water, and health care to the citizenry, trade, and the production of goods and services.

The recovery of any one of these key national infrastructures is dependent on others working. We have a very tightly integrated, high-efficiency, mutually interdependent set of national infrastructures. The longer the basic outage, the more problematic and uncertain the recovery of any of these infrastructures will be. It is possible, indeed, seemingly likely, for sufficiently severe functional outages to become mutually reinforcing until a point is reached at which the degradation of a set of infrastructures could have irreversible effects on the country's ability to support any large fraction of its present human population.

EMP effects from high-altitude nuclear explosions are not new threats to our Nation. The Soviet Union in the past, and Russia and other nations today, as Dr. Pry has just masterfully summarized, are capable of creating these effects. Historically, this application of nuclear weaponry was mixed with a much larger proportion of nuclear explosives that was the primary source of destruction, and thus, EMP as a weapons effect was not a primary focus of U.S. defensive preparations. Throughout the Cold War, the United States did not try to protect its civilian infrastructure against either the physical or an EMP effect of nuclear weapons and instead depended on deterrence for whatever safety might be attained.

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

Single detonations of certain types of relatively low-yield nuclear weapons can be employed to generate potentially catastrophic EMP effects over wide geographic areas, and designs for variants of such weapons may have been illicitly trafficked for a quarter century. I refer specifically here to what Dr. Pry labeled as super-EMP.

China and Russia have considered limited nuclear attack options that, unlike their Cold War plans, employ EMP as the primary or sole means of attack, as indeed Dr. Pry noted. As recently as May 1999, during the NATO bombing of former Yugoslavia, former high-ranking members of the Russian Duma, meeting with a U.S. Congressional delegation to discuss the ongoing Balkans conflict, raised the specter of a Russian EMP attack that would paralyze the United States. Open source Chinese military writings have de-

scribed, in the event of a conflict over Taiwan, using EMP as a means of deterring or defeating the United States, all as Dr. Pry has raised before you.

The key difference, the Commission found, from the past is that the United States has developed more than most other nations as a modern society. It is heavily dependent on electronics, telecommunications, energy, information networks, and a rich set of financial and transportation systems that critically leverage modern technology. This asymmetry, already large and growing even larger, is a source of substantial economic, industrial, and societal advantages, but it creates vulnerabilities and critical interdependencies that are potentially catastrophic to the United States.

Therefore, terrorists or state actors that possess relatively unsophisticated missile armed with nuclear weapons may well calculate that, instead of destroying a city or a military base, they may obtain the greatest political-military utility from one or a few such weapons by using them, or by threatening their use, in an EMP attack. The current vulnerability of critical U.S. infrastructures can both invite and reward such attacks, if not corrected. As Secretary of Defense Don Rumsfeld has said, vulnerability invites attack, to which I might add that extreme sustained vulnerability entices such attack.

However, correction is feasible and well within the nation's technical means and material resources to accomplish. Most critical infrastructure system vulnerabilities can be reduced below those levels that potentially invite attempts to create a national catastrophe. By protecting key elements in each critical infrastructure and by preparing to recover essential services, the prospects for a terrorist or rogue state being able to impose large-scale long-term damage on the United States can be minimized. This can be accomplished reasonably and expeditiously.

Such preparation and protection can be achieved over the next several years given a well-focused commitment by the Federal Government and readily affordable levels of resources. We need to take actions and allocate resources to decrease the likelihood that catastrophic consequences from an EMP attack will occur, to reduce our current serious levels of vulnerability to acceptable levels and thereby reduce incentives to attack, and to remain a viable modern society, even if an EMP attack occurs. Since this is a matter of national security, the Commission felt strongly that the Federal Government must shoulder the responsibility of managing the most serious infrastructure vulnerabilities, including resourcing the timely obviation of these vulnerabilities.

Homeland Security Presidential Directives 7 and 8 lay the authoritative basis for the Federal Government to act vigorously and coherently to mitigate many of the risks to the nation from terrorist attack. The effects of EMP on our major national civilian infrastructures lie within these directives, and the directives specify adequate responsibilities and provide sufficient authorities to deal with civilian sector consequences of an EMP attack.

In particular, the Department of Homeland Security has been established, led by a Secretary with the authority, responsibility, and the obligation to request needed resources for the mission of protecting the U.S. and recovering from the impacts of the most seri-

ous threats. This official must assure that plans, resources, and implementing structures are in place to accomplish these objectives, specifically with respect to the EMP threat. In doing so, the Department of Homeland Security must work in conjunction with other governmental institutions and with experts in the private sector to efficiently accomplish this mission. It is important that metrics for assessing improvements in prevention, protection, and recovery be put in place and then evaluated, and that progress be reported regularly and independently reviewed.

Specific recommendations are provided in the EMP Commission's report with respect to both the particulars for securing each of the most critical national infrastructures against EMP threats and the governing principles for addressing these issues of national survival and recovery in the aftermath of an EMP attack. Much of the problem can be addressed very economically without major capital investments, but by developing effective plans to meet the challenges posed by EMP threats.

For example, one major Commission finding is that the electric power grid is the keystone infrastructure upon which all other infrastructures vitally depend. Yet today, there is no plan for black-starting the national power grid in the event of a continent-wide collapse of the system. If the electric power grid can be quickly recovered, the other infrastructures can be recovered adequately in the aftermath of an EMP attack. Conversely, if it cannot be quickly recovered, most, if not all, of the other infrastructures will not only collapse, but they will be exceedingly difficult to ever bring back.

Making the key aspects of the nation's infrastructure more robust against EMP attack ill also pay dividends by protecting against other types of large-scale problems with them, such as natural disasters.

This concludes my statement, Mr. Chairman. I invite your attention and that of your colleagues to the fact that several critical findings and recommendations of the Commission can be conveyed properly only in closed session. Again, my colleagues and I thank you for the opportunity to report the findings and recommendations of the EMP Commission to the United States Senate.

Chairman KYL. Thank you very much, Dr. Wood and other members of the Commission.

[The prepared statement of Mr. Wood appears as a submission for the record.]

Chairman KYL. I am going to quote just three sentences from your testimony, especially for those in the media. I think if you are looking for a take-away, here it is. "The bottom line is that several classes of potential adversaries, including terrorist groupings, have or can acquire the capability to attack the United States with a high-altitude nuclear weapon generated electromagnetic pulse. A determined adversary can achieve an EMP attack capability without having a high level of either military or nuclear sophistication. The effects on the systems and infrastructures dependent on electricity and electronics could be sufficiently ruinous as to qualify as catastrophic to the nation."

I guess the final point would be that you indicate that there are recommendations the Commission has made which, if implemented, could ameliorate the effects of this, and I want to get into

that. But those three sentences, I think, illustrate the reason why it is important not to succumb to a failure of imagination again and for this Subcommittee to continue in its effort to identify potential kinds of terrorist threats that we need to look at.

What I would like to ask in my series of questions, and any of the three of you should feel free to jump in here, it seems to me that for an amateur, we need to look at it this way. First, what exactly would an EMP attack do? Why might terrorists use EMP, and how would they do it? And what could we do about it? Those are kind of the three key questions.

First of all, and I will probably start with—well, all three of you actually can discuss this, although I am not sure, Dr. Fonash, whether you want to get beyond the telecommunications area. If you do, feel free.

Mr. FONASH. Sir, I would like to restrict my comments to predominately telecommunications—

Chairman KYL. Okay.

Mr. FONASH.—and not discuss threat at all, and some of your questions address threat and that is more appropriate for DOD or CIA to address those questions.

Chairman KYL. Right. Well, I will just ask you to jump in then when you want to, if you would.

But with respect to what an EMP attack would do, my own amateur view is that it would just fry all the electronic circuits and everything we have and I can't imagine hardly anything in our society that isn't controlled by some kind of a pump or a computer or communication of some kind or other. Would one of you be just a little bit more specific about—just paint a scenario of what would happen when this nuclear device exploded in the atmosphere, generates these pulses that come down on earth, as you have it right there over my home town of Phoenix, Arizona.

Mr. WOOD. Mr. Chairman—

Chairman KYL. And, excuse me, just bearing in mind that we have a nuclear generating plant there, we have Hoover Dam right outside, between Phoenix and Las Vegas there, as well as a whole lot of other kind of facilities that I am sure you can imagine.

Mr. WOOD. Mr. Chairman, the first thing that needs to be made clear is there has never been a large-scale EMP attack on any site anywhere, ever. So there necessarily is a large component of extrapolation from the measurements that have been made from the high-altitude nuclear tests. And those measured features have been taken into quasi-laboratory environments and there, various types of equipment, both military and, under the auspices of the Commission, a great deal of civilian equipment has been subjected to the measured circumstances that are created by a high-altitude nuclear detonation.

Then another large measure of extrapolation is made from the damage to functionality and the physical damage that is seen to be imposed in those laboratory circumstances to what would happen if those circumstances were applied all over a country or over a large region.

So there are two major aspects of extrapolation between measurements that were made primarily in the early 1960's and what we believe would happen if an EMP attack was imposed on a coun-

try or a large region thereof. So those are very important qualifications, and that is why there can be some ground for discussion between technical experts on precisely what the circumstances would be, two large sections of extrapolation.

The Commission's findings, after listening to all of the experts, sponsoring a great deal of work on its own, which had never been done for the civilian infrastructure previously, was that the effects can be anywhere from highly transient, highly localized geographically, and a mere annoyance of the scale of a large electric power blackout. That is on the low end. On the high end, the consequences would be loss of major national infrastructures over the entire continent for an indefinitely great period.

Where things fall in the spectrum in between these two extremes depends critically on the nature of the explosion, the place at which it is conducted geographically, the altitude at which it is conducted, the type of explosive which is used, which was determined by the Commission both on its own and with substantial foreign inputs to be an exceedingly critical parameter, and finally, on the degree of preparation that is taken against the consequences of such an attack.

So this is an area which, to use technical jargon, the parameter space is kind of as big as all outdoors. It goes all the way from, as I said, the consequences of a blackout, which might have economic, as we saw a couple of years ago, might have economic scales of $20 billion, in round numbers, and essentially no loss of life, just a great deal of inconvenience, to something which would literally destroy the American nation and might cause the deaths of 90 percent of its people and would set us back a century or more in time as far as our ability to function as a society.

Chairman KYL. Now, with respect to that latter kind of a threat, a lot of things would have to be coincident. You would have to have a dramatic set of circumstances, the right kind of weapon, the right altitude, and all of the other factors. But take that most serious case, or something somewhat less than that, and describe specifically the kinds of things that would physically occur. What physically occurs to the infrastructure of Phoenix, Arizona, in that event, or the State?

Mr. WOOD. What happens is that a nuclear explosion is caused to occur at a significant altitude, a few dozen to a few hundred kilometers, by any means that can be arranged for. One of the means that might concern us very much at the present time is a Taepo Dong-2 missile carrying an advanced nuclear warhead from North Korea.

One of the striking things that you heard today from Dr. Pry, which has not been tabled previously in public, is that North Korea should not be considered as just potentially possessing first generation nuclear weapons, but potentially the most advanced nuclear weapons that exist on the planet because they have received a great deal of foreign assistance.

So when we stop to think about being attacked from North Korea, we shouldn't think about Hiroshima or Nagasaki. We should think about flavors of destruction that have never been seen before on this planet.

Chairman KYL. Well, taking—

Mr. WOOD. So when that—

Chairman KYL.—taking that kind of weapon, what physical—

Mr. WOOD. When that type of weapon is exploded at several dozen to a few hundred kilometers above the United States, if it happened in the middle of the day, you might see or hear nothing. The lights would go out. A great deal of things instantly dependent on electricity would go away. And depending on the nature of the damage, its severity, its geographical descent, the lights might come back on hours later, they might come back on decades later.

If they come back on in hours, as we know from blackouts, there is just a great deal of inconvenience and substantial economic loss. If the lights stay off for more than a year in this country, the Commission's estimate was the loss of life would run into the tens of millions, perhaps a great deal more. You miss the harvest. You have no refrigeration, no transportation, no anything except what we had as a country in the 1880's. Most Americans will die in that interval.

Chairman KYL. Well, how much of our country, and maybe I can ask Dr. Pry to answer this, how much of our country depends upon some kind of electrical system working?

Mr. PRY. Our entire country depends on some type of electrical system working. If I could add to what Dr. Wood has said about what the effects would be, what it might be like, one should think about the kinds of blackouts that happened in the aftermath of hurricanes, for example. In addition to the other data that he talked about, the Commission also sponsored studies that took a look at the consequences of major blackouts that were induced by storms—ice storms, hurricanes, that sort of thing.

We tend to think of those as fairly commonplace because they tend to be isolated geographically and there is something called the edge effect, because they will effect—for example, Hurricane Andrew affected eight counties in Central Florida, and so we had the entire rest of the country was unaffected and we were able to come in and recover from that very quickly.

But if you look at what happened in those eight counties, there was no food. There was no water. There was no communications. People couldn't even communicate to find where they could go to get food and water. There were rippling societal consequences where there was basically a breakdown of law and order and it became a chaotic situation where the National Guard had to be sent in to—

Chairman KYL. You said they couldn't communicate. What would happen with the electromagnetic pulse that would prevent communication?

Mr. PRY. Well, it would knock out—first, it knocks out the power grid, so there is no electricity to run televisions, for instance. Most people don't have battery-powered radios anymore. Most of the radios that are around depend on electricity. Everything depends on electricity.

Transportation was paralyzed in that area because the traffic lights couldn't work.

Chairman KYL. Could you pump gasoline?

Mr. PRY. You couldn't pump gasoline. You basically had only as much as gasoline as was available in the tank of your car. This

happened during the August blackout in New York, as well. You saw these same infrastructure failures passing off, flowing from the failure of the electric power grid, collapsing like dominoes, each of the infrastructures, including the telecommunications infrastructure. It didn't become a catastrophe because of the edge effect, because we were able to move in there, and also because it was just the power grid that was down, in the case of New York, and so fairly easily repairable. It could be repaired in a week or two.

But if you extrapolate something like that happening for months or years, you are obviously talking about a life-threatening kind of a catastrophe because you cannot endure, or you cannot support the population without food, without water for those protracted periods of time, nor can one count on societal stability for protracted periods of time. I think the Andrew experience in those eight counties, what happened there in terms of social cohesion is instructive in terms of what could happen on a national basis if such a disaster were to occur.

And you don't need the—and I completely concur with Dr. Wood about the range of uncertainty that exists in these things, but we ought not to take—he was talking about the super-EMP. The thing is, we don't know how low down you can go with that threat. It might well be that in order to achieve these things, it may be possible that even without a super, with a first generation weapon, you might be able to do it.

And the reason for this is the keystone infrastructure is the electric power grid. When that collapses, the rest of the infrastructures are going to collapse, as well. And the electric power grid, as we learned from New York, is always operating on the edge of failure. It is old. It has not been modernized and updated. In Commission work, there are cases where a falling tree branch has caused a multi-State blackout that has lasted a week.

Chairman KYL. Let me—

Mr. PRY. If a falling tree branch can do that, a first generation atomic weapon, I hate to think what that could do.

Chairman KYL. And I want to get to the kind of weapon that might be used and how a terrorist group might want to do that. Let me just ask one last question. In Phoenix during the hot part of August, there was a fire at a switching station for one of the utilities and two transformers were burned. We were on the edge of a catastrophic failure in Phoenix because of that because the only place where the transformers could be purchased, I believe, was someplace in Italy. It took a long time to get them there and they had to be transported by a very large, special kind of truck. Thankfully, we had enough generation and transformer capacity to just barely work out of the problem. But would a nuclear weapon cause damage to things like switching facilities, transformers, as well as other kinds of circuitry?

Mr. WOOD. Mr. Chairman, I think the situation that you just described is existing in most, if not every, city across the country. If the United States was subjected to a continental-scale EMP attack, you would see damage of the type that you describe, but of a much more serious character, to all of the major transformers at once that are connected and that are postured so that they would see

not the instantaneous component, but the slow or several-minute duration component.

This is not hypothesis. This is the type of damage which is seen to transformers in the core of geomagnetic storms. The geomagnetic storm, in turn, is a very tepid, weak flavor of the so-called slow component of EMP.

So when those transformers are subjected to the slow component of the EMP, they basically burn, not due to the EMP itself but due to the interaction of the EMP and normal power system operation. Transformers burn, and when they burn, sir, they go and they are not repairable, and they get replaced, as you very aptly pointed out, from only foreign sources. The United States, as part of its comparative advantage, no longer makes big power transformers anywhere at all. They are all sourced from abroad.

And when you want a new one, you order it and it is delivered—it is, first of all, manufactured. They don't stockpile them. There is no inventory. It is manufactured, it is shipped, and then it is delivered by very complex and tedious means within the U.S. because they are very large and very massive objects. They come in slowly and painfully. Typical sort of delays from the time that you order until the time that you have a transformer in service are one to 2 years, and that is with everything working great.

If the United States was already out of power and it suddenly needed a few hundred new transformers because of burnout, you could understand why we found not that it would take a year or two to recover, it might take decades, because you burn down the national plant, you have no way of fixing it and really no way of reconstituting it other than waiting for slow-moving foreign manufacturers to very slowly reconstitute an entire continent's worth of burned down power plant.

Chairman KYL. Let me now switch to a different inquiry. Terrorists are very clever, but sometimes it seems to me they are more interested in something really showy than something that might be even more damaging. I am presuming something that I don't know here, and a smart terrorist just might figure that this is exactly the thing that he wants to try to achieve. But I always thought that if there were access to a nuclear weapon, that the biggest bang would be to blow up a whole lot of Americans in a city, cause the collateral damage, but primarily the immediate loss of lives.

So the first question that came to my mind is, while I could understand in war or preparation for war a power, and just to use a hypothetical case like China, for example, or North Korea, might want to freeze our capabilities with an EMP kind of attack, would a terrorist necessarily turn to that as the first choice? And then, of course, the response comes in, well, maybe that is not a matter of choice, but it is a matter of convenience. What were the scenarios that the Commission looked at that led it to conclude that this might well be doable and something that a terrorist would actually decide was the best thing to do or the only thing that could be done?

Mr. WOOD. Mr. Chairman, the Commission proceeded not on a scenario-driven fashion but on a capabilities-based manner, and so we looked at the capabilities that would have to be brought into existence by an attacker to impose various levels of damage and we

tried to steer fairly clear of sketching ways, particular ways in which particular people might choose to do this because, frankly, thinking like a terrorist or thinking like a rogue state leader or whatever is well outside the competencies that the individual Commissions brought. None of us have been terrorists and very few of us have led rogue states, and so we merely looked at the capabilities that could enable such behaviors.

Chairman KYL. Not inviting a comment about Berkeley there.

[Laughter.]

Mr. WOOD. So the inflow bottom line, or line that we drew across the bottom of our considerations is that we wouldn't look or worry about capabilities that didn't impose at least $100 billion worth of damage on the United States in a stroke and went on up from there.

The damage to the infrastructures that we contemplated went on up into $10 trillion scales—trillion dollar—that is to say, a large fraction of the total capital value, capital plant value of the United States as a nation. The thing which is impressive to us is that nuclear explosives and ballistic missiles to carry them up to altitude costing of the order of a million dollars could potential impose $10 trillion worth of damage. That is to say, ratchet it up by something of the order of a factor of $10 million-fold. That was extraordinarily high leverage.

Now, terrorists might be very much inclined towards attacking iconic targets, but if it is a semi-rational terrorist, he probably looks for leverage and one of the types of leverage that is probably most impressive is dollar leverage. How much can I destroy per what I invested? Osama bin Laden boasted of how little he spent on the attack on the Twin Towers and how much damage was imposed and so forth. So at least some senior terrorists think in those terms, think in terms of return on investment, if you will, and/or at least their financial backers think in those terms, and so it didn't seem totally inappropriate to look at, well, what could be done with a single or a very small number of weapons that could be purchased or otherwise obtained for very reasonable values on the world market?

There is roughly 35,000 Scud ballistic missiles, for instance, in existence at the present time. As I said, they sell for a small fraction of a million dollars apiece, and private collectors in the continental United States have taken delivery as private individuals on Scud missiles in their homes that were in operational condition. So these things are easy to come by. Probably the most challenging thing from a terrorist's standpoint is getting either an ordinary nuclear weapon for an ordinary EMP or an advanced one for super-EMP and getting somebody to launch it from Canada, Mexico, tramp freighters off the coast, any of many places where an attack of at least a regional character, if not a national character, could be pressed against the United States.

Chairman KYL. I realize that you all are very scientific and precise in your approach to these problems, and you caveat your conclusions very carefully, that you are not into scenario analysis. But with respect to the average person thinking about how, not how likely it would be, but at least whether there is some remote possibility that this could occur and, therefore, it would be something

that we would want to put assets against to try to protect against it or to deal with it if it occurred, there has to be some element of probability involved.

And so one gets into questions of how easy it would be, for example, for a terrorist organization, as opposed to a state, to launch a guided missile against a specific target in the United States with a nuclear warhead on it and whether that would be just as easy to do as detonating something in the air that would cause this kind of damage.

You pointed out that the range of missile available to a terrorist would not be an ICBM today, presumably, but would be a shorter-range missile so that it would have to be launched from something off our coast or in an adjacent area. But as you note in testimony and as Dr. Pry noted, that could come from a seaborne vessel from which Scud-type missiles have been successfully launched, is that correct?

Mr. WOOD. Indeed, the Secretary of Defense has pointed out twice in the last year and a half that at any given time, any of a couple of dozen vessels off the coast of the United States count mount such an attack, and those have been, as I pointed out, kind of off-the-cuff statement in news conferences as, hey, everybody understands and knows that.

Chairman KYL. Yes.

Mr. PRY. If I could add to what Dr. Wood has said, al Qaeda is known to own 80 freighters. I think that is the estimate. They are supposed to own 80 freighters. The Scuds, some models, the Scud-1 can be purchased for $50,000. So that is well within their capability. The hard part is the nuclear weapon.

If you had a Scud and a freighter, would you attack a city to kill people versus doing the EMP? Well, one problem you have with that mode of attack for going against the city is that it is so inaccurate that the likelihood is, well, you are running a great risk that you might not hit the city at all. That isn't a problem with the EMP because the area of effect is so great that all you have to do is just get it up to the proper altitude. So that technical consideration might well tend to—

Chairman KYL. This is a very important point that I would like to just have us dwell on for just a moment, because it does help to answer the question of why potentially an EMP attack. I mean, one answer is you are very rational and you know how to leverage money and to get the most bang for the buck, Dr. Wood's testimony earlier. The second reason would be that it might be very difficult to launch a missile with the kind of guidance available for a Scud missile, for example, to actually hit your target in the United States if you were doing this from a barge or a freighter offshore, is that correct?

Mr. PRY. Oh, yes, and there is additional considerations. You know, a missile that is going to go to ground, to actually hit a city, is going to be more vulnerable to missile defenses than an EMP. An EMP only has to complete half its trajectory, and doing it the other way, to go after a city, has to complete its full trajectory, and at the end of the trajectory is exactly when you are going to be most vulnerable to missile defenses.

And look at what are you trying to accomplish? Suppose you had a first generation weapon. Suppose you, instead of using a missile, suppose you had a suitcase-type thing or you wanted to send it into New York Harbor or something like that. Well, with a 20-kiloton weapon, you are not going to destroy the City of New York. You will kill a couple of hundred thousand people and then pray that the United States doesn't find out who your state sponsor was, because then we would turn that state sponsor into a plate of glass. With EMP, you at least have a possibility of actually killing millions of people, millions of people, and getting a much bigger bang for the buck.

Moreover, whereas the attack on a city could backfire in the sense of instead of breaking the will of the American people in the war on terrorism, it could just further enrage us and steal our resolve to project our military forces and use our strength to prosecute that war, when you think of, well, how could the terrorists possibly win the war on terrorism, this is one of the few options that is available for them to actually win the war on terrorism. If they could destroy the United States as a superpower by disrupting our infrastructures, they would win the war on terrorism.

Perhaps this is why Iran is doing the kinds of tests it is doing with those Shahab-3s that have been burst at high altitude. We have described them as test failures. They have described them as successes, as I alluded to in the testimony. And why do that test off of a freighter?

And we also know from al Qaeda that Osama bin Laden, one of the reasons he attacked the World Trade Centers was financial. They were hoping to disrupt our economy. That was one of their goals. It isn't just to kill people, it is to do as much damage as they can to us, including economically and financially.

Mr. WOOD. Returning to your core thrust just briefly, Mr. Chairman, the basic thing that should intrigue an attacker, a rational attacker, about mounting an EMP attack is, as Dr. Price said, you only have to do half of the normal ballistic missile mission. Two things that are crucial that were cited by implication that deserve to be emphasized is that you only have to throw the payload up. That is the essence of the thing. You aren't concerned at all with precision targeting, and very importantly, when you come down, you have to face the so-called atmospheric reentry problem, which can be quite challenging, particularly for a longer-range, higher-speed missile.

EMP attacks don't have to cope with that at all, so they throw away at once the requirement to cope with missile defenses, that is terminal phase missile defenses. They don't have to have good guidance. They don't have to have reentry systems. They literally can be a Fourth of July-type rocket with a nuclear explosive on the front. And so that is a set of enabling things which make an attack much, much easier to launch.

And then when you start looking for telltale features and so forth, this combination of launching off a barge in the Caspian, what in the world motivation does the Iranian government have for launching off a barge against Israel, against Iraq, against any of its traditional local enemies? Launch off a barge? It makes no sense at all. What sense does it make to have your test detonate

its payload at high altitude in mid-course? No sense whatsoever, and yet they do this. So you either say they are crazy, which is the lazy way out, or you say, what in the world are they intending to actually do?

Chairman KYL. So before we get to how do we fix this problem, then, we have got sort of the means and the motive pretty well established as well as a huge amount of damage should such an attack occur. We, therefore, get to the question of what can we do about it and there has been work done on this both in terms of the Department, as Dr. Fonash discussed, as well as the recommendations that the Commission made in its report.

Perhaps we could spend just a little bit of time on that, because we don't want to leave people too afraid that we are going to wake up tomorrow morning with a huge problem on our hands here. What are we doing about it? What can we do about it?

Mr. WOOD. I would just like to, before we leave the first section, Mr. Chairman, to comment that the Commission's report to the Congress is in three basic segments. One is the Executive Summary and the main body of the report, all of which are unclassified or in the late stages of being formally declared to be unclassified. We hope to see that out entirely very soon past the executive branch reviews.

The second main piece is concerned with military matters, which the Commission was charged with looking at military vulnerabilities, as well. That report is classified secret and is available through appropriate channels at the present time.

The third one, which is classified top secret with special caveating and labels and so forth that would typically go with intelligence matters, addresses specifically the points that you referred to, from whence is the attack coming and when and how soon and with what likelihoods and why would people be motivated to be doing it and what are they actually doing. That is very highly classified and that report and its findings and recommendations obviously can be addressed only in closed session. That is what I referred to in my opening statement. But there is a great deal of information that was examined by the Commission and assessed and findings and recommendations based on it in that final relatively small portion of the report, which necessarily is discussed only in very cloistered circumstances. But it is discussed.

Chairman KYL. Dr. Pry, would you like to perhaps first address the problem, the recommendations of the Commission?

Mr. PRY. Yes. Ultimately, this is really a good news story. Despite the catastrophic nature of the threat, I think one of the breakthroughs the Commission really did—made—it came up with, in a sense, a blueprint that, if followed, in three to 5 years, at affordable, modest cost could mitigate, so mitigate the effects of the EMP threat that we could take it out of the catastrophic category and recover from this particular threat. That is a huge accomplishment.

You can't say that about the other handful of threats that could destroy us as a society, like genetically engineered smallpox, for example. Things like that are still such a formidable problem, most people are still trying to get their arms around how to solve it. But this one is doable.

Much of it involves common sense. For example, those transformers Dr. Wood referred to, instead of having the ability to replace only 1 percent of the transformers in this country, which is about what we have got now, maybe we should have about 150 of these transformers purchased in advance, stored on-site in metal sheds that are welded in such a way that they become cages so that they would be protected from the effects of EMP, disconnected from the power grid. Then you could quickly replace those transformers, and as we found from our analysis, once you get that power grid up, you can bring back all the other infrastructures fairly expeditiously. That wouldn't cost that much. That could be accomplished in three to 5 years.

There are other things that don't involve buying anything, but it is just a case of thinking about it and planning. Take diesel-electric locomotives, for example. There are tens of thousands of them in this country. Each diesel-electric locomotive, they can generate about a megawatt of electricity. In Canada, for years, they have been using them during the winter to power villages and small towns. That is how much electricity you get out of one of these things.

We are taking the wheels off and sending them to Iraq, American diesel-electric locomotives, to supplement the destroyed electric infrastructure over in Iraq. Maybe we need a plan in the aftermath of an attack like this, or a cyber terrorist attack or something else that would interfere with our power grid, to take advantage of the tens of thousands of diesel-electric locomotives. Where do we drive them to? What are the highest priority things?

I would suggest maybe we need to drive them to those regional food warehouses, the larder of the United States. There are maybe a couple of hundred regional food warehouses in which a 60-day supply of food, you know, supplies all of the States. In the supermarket, you have only got about a day or two worth of food. Where the food comes from, it is transported by truck from these regional storehouses which critically depend on refrigeration and temperature control, so the food will spoil very quickly. Maybe we need to get diesel-electric locomotives to each of these things to keep them powered up, and to hospitals and to other critical nodes in communications and in the power infrastructure so that we can most expeditiously bring things back in that aftermath.

The Commission found another example. There is a particular fuse that is just by accident of its design that is much less susceptible than the fuses that are currently used in traffic signals, to control traffic lights and other kinds of traffic regulation. This fuse costs, like, one penny more than the fuse that is currently used, but is much harder to the effect.

So these are just some examples of things that would go very inexpensively a long way toward mitigating the problem. I would underscore most of all, though, the big transformers and the fact that I don't think we can afford to be dependent on a foreign country, not have reserve transformers in this country to bring back our power grid.

Chairman KYL. We will talk about communications in just a second, but I can think of so many other problems that could arise. In order to pump water, you have to have electricity.

Mr. PRY. Yes.

Chairman KYL. You could get into a fire situation or other situations in which you could have a conflagration that you couldn't deal with because you couldn't get water on it or other kind of fire retardant, for example.

Mr. WOOD. Indeed, the Commission found that just exactly that problem was likely to be an exceedingly serious one, sir, in the immediate aftermath of an EMP attack, that the fires, once started, would spread completely out of control and without human intervention, effective human intervention, something for a lack of ability to source water onto those fires, create fire breaks, and so forth. So that is the sort of immediate aftermath.

If a terrorist wanted to have something iconic happen as a result of an EMP attack, it would be that in a matter of hours after a very large-scale attack, America's cities would be in flames and they would burn until they burned down. And in the following few days, as people were unable to get food in markets and so forth, four million Americans under the age of 1 year of age would die of starvation because there wasn't infant formula and the other specialty items that people are used to always finding in stores, so they need them. Young children are very fragile and we would lose four million infants under the age of one in the first two weeks, most all of them, and so forth.

So the damage would be pretty dramatic. Nobody gets killed right away, but in the immediate aftermath, America in a lot of senses would be hammered to its knees unless, and this is a crucial—excuse me, sir—unless, as Dr. Pry pointed out, and this was a key finding of the Commission, the attacks were regional and the edge effects could be martialed very, very swiftly and effectively so that the rest of America came to the rescue of the portion that had been brought under.

Chairman KYL. But for that, we have to start with a plan.

Mr. WOOD. Of course. We have to not only have the plan, but we have to have the things to enable the plan very quickly.

Chairman KYL. Right. Now, do any of you know whether the recommendations of the Commission have been dealt with in any specific way by the Department of Homeland Security? Leave out Department of Defense, because that is really a different issue.

Mr. FONASH. Let me answer that in two ways. First of all, let me talk to you about telecommunications and then let me talk about DHS infrastructure protection in general.

Chairman KYL. Thanks.

Mr. FONASH. With regards to telecommunications, we have participated, the Commission, we actually testified in front of the Commission. As I said before, for over 20 years, we have been testing equipment against EMP and other electromagnetic effects. So we are very well aware of the Commission's recommendations. We have implemented many of those recommendations. And we also continue our testing program. We remain vigilant in communications against the EMP threat or any other type of EMP or electromagnetic effect against telecommunications.

Telecommunications basically is the—the telecommunications infrastructure we have today is relatively impervious to EMP. It would be disrupted, but then it will be restored. It can be restored.

There is a dependency of our telecommunications infrastructure on power, but that is an dependency that we are aware of and we are working at. And during a blackout, going to the New York blackout, communications functioned well. The basic communications worked through the blackout, and that is due to the fact that major communications centers have multiple sources of back-up power, one being that they have battery back-up, and then in addition to battery back-up, they have diesel generators.

Now, of course, there is a dependency on the diesel generators on fuel, and so eventually, if you don't get the diesel generators refueled, there would be a problem. But during a blackout in New York, the telecommunications basically functioned.

Now, with regards to the overall issue, is the Department of Homeland Security addressing this, since the creation of the Department of Homeland Security in 2003, we have been trying to protect our critical infrastructures, and what we have done is we have created the interim National Infrastructure Protection Plan consistent with Homeland Security Presidential Directive 7, which directed us to develop a process to protect our critical infrastructures. And the interim National Infrastructure Protection Plan really lays out a framework, a risk management framework and a process for protecting the 17 infrastructures of this country, and I speak for only one of 17, but there are 17 infrastructures.

DHS, in our role of the National Infrastructure Protection Plan, we provide leadership across the infrastructures. We coordinate across the infrastructures. We develop process and tools. And we are the sector leads in certain infrastructures, for example, telecommunications, but we also work in interdependencies. Interdependencies cross infrastructure. For example, interdependency of other infrastructures on power is an example.

But we put in the process. We are identifying the assets. We want to assess those vulnerabilities of those assets. We are going to prioritize those assets in terms of the impact of any damage to those assets with those vulnerabilities, and then we will protect and we will establish metrics.

And I want to say, so those are the things that we have put into place and we seek input in terms of vulnerabilities from all sources and we would certainly consider the Commission's report while we work with DOE, who is the sector lead for energy, as they develop their sector plan for how they plan on protecting the energy infrastructure.

Chairman KYL. Dr. Pry?

Mr. PRY. I respectfully disagree with my colleague that the telecommunications infrastructure is as robust as is described against the EMP effect. This is a nether card, which is an example. It is ubiquitous. There are millions of these in the communications infrastructure. The Commission sponsored testing against a moderate level of EMP and it was damaged. The damage is indicated by the arrow that was indicated here. To have massive failure of this kind of an item would be a very serous blow to our communications infrastructure.

The blackouts example that was referred to, the blackouts, of course, lasted only a short period of time, and while it is true that there are nodes in the communications infrastructure that have

generators, one of the things I wanted to comment on when you raised the issue of fire is that we found it to be the trend that is happening in terms of the robustness of these generator facilities and battery facilities. It is actually going in the wrong direction. There is a tension between the—in the fire codes, a concern about storing large quantities of flammable petroleum products to run these generators, and in many cases, in many cities, they are scaling back on the amount of petrol that is allowed to be stored for the generators. So the time that you can run these generators is getting less and less when really, the trend probably, if you take EMP seriously as a threat, ought to be going in the other direction to give you a more protracted capability to generate electricity.

Mr. WOOD. If I could interject there just very briefly, Mr. Chairman—

Mr. PRY. The problem is not just simply fuel storage, which the Commission found was indeed an alarming trend, and that it is not only going in the wrong direction, but it is going in the wrong direction very rapidly in that not only are the allowed fuel depots becoming smaller, but even the permission to start and operate the emergency generator systems is being strongly circumscribed by air pollution considerations. You literally can't run these systems for more than very brief intervals without having a variance on your operating permit to allow you to go on for four hours or eight hours.

Mr. WOOD. There is very substantial concern that the apparent ability to backup electric power for the communications system is simply illusory and is becoming more so very swiftly. Excuse me. Go ahead.

Mr. PRY. If I could continue, a third point is the super-EMP weapon, okay. What are you robust and hardened against? The notion of this new technology is basically a discovery of the EMP Commission. It was a consequence of reviewing foreign military writings and actually meeting with foreign military officers that there is a technology out there which our own experts have looked at and consider highly plausible and that this might already have been weaponized.

The threat, the wave form, both the strength of—the field strengths that you are talking about and the wave form are very different from those that we were thinking about during the Cold War. We can't really get into it in great detail here in this unclassified forum, but that is a new threat, and so how could one be confident that you are robust against that threat that we are only now just beginning to understand?

And last, in terms of the familiarity, I suppose it is possible to be familiar with the Commission's recommendations, because I know some of our Commissioners have worked with—have talked to people from Homeland Security, but the fact of the matter is that Volume 3 of the Commission report, which is where the detail about our recommendations is, is not available to any agency or department yet. I mean, it is still going through the security classification review process and hasn't been issued yet.

So I can see how one might know about some of the recommendations generically from the Executive Summary, and then perhaps gotten some detail from some of our Commissioners, but

I have to be kind of skeptical about the idea that there is great familiarity with a report that has not yet been delivered to either the Department of Defense or the Department of Homeland Security.

Chairman KYL. Is there a specific process by which the Commission believes it can be in communication with the appropriate agencies, primarily DOE, DOD, and DHS, and a process, then, of review and action for planning would follow? Is there a fairly clear path there, or is that something probably that we should help to create and foster?

Mr. WOOD. Mr. Chairman, the Commission, as specified in the statute, is a creature of the Congress—

Chairman KYL. Right.

Mr. WOOD.—and it is an advisory body to the Congress. It had input from the executive branch primarily in the way the individual Commissioners were appointed by the Secretary of Defense, primarily, and also by the Director of FEMA, now a part of DHS. But the specification was—the mandate to the Commission was to assess, find, recommend, and report, and that is what we are doing, and to the extent that the Congress has in mind activities or responsibilities beyond that, they need to instruct us.

Chairman KYL. I think probably with your advice, and I will be in touch with you and will certainly be in touch with DHS, as well, probably try to put together a letter to all of the various heads of the departments concerned with a request that as soon as the—well, to transmit the reports as they currently are and make sure that as they are each completed, at the appropriate levels of classification, that they are transmitted and that a process for agency interaction and response be created with a report back to the Congress. If that hasn't been done by anyone else in the Congress, I will pursue that.

Dr. Pry?

Mr. WOOD. Mr. Chairman, the basic issue there was that DHS, of course, did not exist when the Commission was mandated—

Chairman KYL. Right.

Mr. WOOD.—in Public Law 106–398, and so it was completely impossible to contemplate DHS being involved. So the Congressional rectification really updating of the arrangements is eminently appropriate there.

We have briefed and we will continue to brief senior officers and officials of the Department of Defense in the portion of the Commission's mandate that was concerned with military systems, but frankly, the key thing that the Commission was to do with respect to vulnerability of civilian infrastructure is dangling at the present time as far as formal arrangements are concerned simply because DHS didn't exist at the time and the Director of FEMA no longer has the responsibilities that the legislation contemplated when the law was enacted.

So the Congress taking the initiative to update the administrative arrangements would be eminently appropriate. It is one of the things that was a basic recommendation of the Commission.

Mr. PRY. If I could add to what Dr. Wood has said, yes, because it does contrast with our relationship with the Department of Defense, where the Commission findings have been briefed all the way up to the Wolfowitz level, to the Navy Secretary. We haven't

had equivalent briefings like that with the Department of Homeland Security. As Dr. Wood points out, Homeland Security didn't exist at the time the legislation was drafted, and so there was perhaps not the legislative obligation or opportunity to have the kind of cooperation that we had with the Department of Defense.

The Department actually participated. I mean, DTRA, the Defense Threat Reduction Agency, we had staff from DTRA that actually participated in our work, was present at all of the deliberations. It wasn't a matter of one or two briefings here and there. They were actually deeply involved in the work of the Commission.

We would hope that a similar relationship could evolve—needs to evolve with the Department of Homeland Security because that is where the primary threat is these days, actually. It is not—there are serious matters in our military forces, too, but primarily, it is a homeland security issue.

Another part of that problem, of course, is that after this Commission delivers its report to Congress, which is going to happen as a consequence of giving briefings like this, its legislative mandate goes away and so the Commission ceases to exist. Over on the House side, and we are hoping to convince people on the Senate side, as well, perhaps this is not a good thing to do at this juncture, that we need to extend the life of the Commission. We have a unique body of expertise here in this Commission and a blueprint that the Commission can help advise Congress on following and help advise the other departments and agencies of the government. We are in the process on the House side of reintroducing legislation to give it a more homeland security kind of direction so that the departments can work together in the same productive way that we have worked with the Department of Defense.

Mr. WOOD. The enabling legislation, sir, includes a mandate to the Secretary of Defense to deliver a report within a year of the Commission's report commenting on the Department of Defense's response and thinking and so on on the issues. Again, because of the lack of currency of the legislation, there is no corresponding mandate to the Secretary for Homeland Security.

Mr. PRY. That is correct.

Chairman KYL. I appreciate all of that. I think this is a propitious time, then, to hold this hearing to not only remind ourselves of the potential for a threat here, but also to get straight what we can do with these recommendations as you conclude your work with the classified version and as you advise the Department of Defense and report back to Congress, as well, how we can also expand the reach of these recommendations to the Department of Homeland Security as well as anyone else like DOE that would need to be aware of them, too.

If that requires a mandate to continue the Commission's work, it sounds to me like that would be a good idea. In any event, informally if not formally, we can certainly direct where the reports should go and set up some meetings so that we can continue to work on the fixes to the problem rather than just identifying the problem and leaving it dangle there.

So unless there is anything else that you all would like to offer, let me just tell you that, on behalf of the Committee, what I will do is get together with my colleagues, draft up an approach to this

issue, the existence of the Commission, the issuances of the reports, both classified and non-classified, the inclusion of the Department of Homeland Security in the process, and anything else that we think we need to do to follow up on these recommendations, and we will communicate with you all and then take whatever action we think is necessary here in the Congress, as well.

Because of my time constraints, if not yours, I am going to terminate the hearing unless there is anything else that any of you would like to add. This has been most informative. We don't mean to scare everybody to death, but by the same token, the failure of imagination, 9/11 Commission report, and it doesn't take much imagination to figure out what could go wrong here. And to the extent that there are some fixes that can be put in place, we need to identify those and get about the business of doing it because this is, in fact, serious business.

Mr. WOOD. Mr. Chairman, I think you have very aptly summarized it. I think the basic thrust, the bottom-line mission from the Commission's standpoint would be that the EMP attack threat is one which is a curious sort of character, that we have prepared to cope with it for decades from a military standpoint, but have, for reasons that I addressed at the outset, didn't much concern ourselves with the civilian implications whatsoever. By doing so, we may have created something of a 21st century Maginot line for the United States, where we are relatively robust in our ability to wage war as far as EMP is concerned, but are exceedingly vulnerable on different fronts which invite, if they don't outright entice, flanking attacks against the American nation.

Chairman KYL. I thank you. For those who might not, again, be familiar with the background of the people who have served on this Commission, I don't think this country could have brought forth a better group of people, a smarter group of people with more expertise in some of the most esoteric aspects of science than the group of Commissioners here. We very much appreciate your service. Some of you have served in so many different capacities this government and our National security. We don't always think of you—I see these fine men and women here in the audience here with their uniforms on and we properly pay them all the thanks that we possibly can for what they are doing on the front line. It is also the fact that we have a lot of folks working here in Washington and elsewhere on very, very difficult problems that also help to ensure our security, and I want to thank all of those people, as well.

So I thank all of you for being here today. We will follow up in all the ways that I think are indicated as appropriate here and see if we can at least provide a degree of security against the threat that we have identified here today. Thank you.

This meeting is adjourned.

[Whereupon, at 4:16 p.m., the Subcommittee was adjourned.]

[Questions and answers and submissions for the record follow.]

[Additional material is being retained in the Committee files.]

SUBMISSIONS FOR THE RECORD

Statement of

DR. PETER M. FONASH

ACTING DEPUTY MANAGER,
NATIONAL COMMUNICATIONS SYSTEM
UNITED STATES DEPARTMENT OF HOMELAND SECURITY

WASHINGTON, D.C.

BEFORE THE

UNITED STATES SENATE COMMITTEE ON THE JUDICIARY

SUBCOMMITTEE ON
TERRORISM, TECHNOLOGY, AND HOMELAND SECURITY

"Terrorism and the EMP Threat to Homeland Security"

MARCH 8, 2005

I. INTRODUCTION

Thank you, Mr. Chairman and distinguished members of the Committee. My name is Peter M. Fonash. I am the Acting Deputy Manager of the National Communications System (NCS). Sec. 201 (g)(2) of the Homeland Security Act of 2002 transferred the National Communications System of the Department of Defense, including the functions of the Secretary of Defense relating thereto to the secretary of Homeland Security. The NCS is aligned within the Information Analysis and Infrastructure Protection Directorate (IAIP) in the Department of Homeland Security (DHS). The NCS is governed under Executive Order 12472 of April 3, 1984, as amended by E.O. 13286, of February 28, 2003, which designates the Secretary of Homeland Security as Executive Agent for the body. As Executive Agent, the Secretary has designated the Assistant Secretary for Infrastructure Protection within IAIP to serve as the Manager of the NCS.

The NCS, as you know, is an interagency body that brings together the telecommunications assets of the Federal government that are of significance to national security and emergency preparedness (NS/EP). Pursuant to E.O. 12472, the NCS is responsible to ensure the existence of a national telecommunications infrastructure that is responsive to the NS/EP needs of the Federal government and capable of providing survivable NS/EP telecommunications services in all circumstances, including conditions of crisis or emergency. However, it is also important to frame NCS' activities relative to telecommunications in the context of other commercial infrastructures and to the interdependencies that exist among them across the nation.

Prior to my recent responsibilities as Acting Deputy Manager, during my almost seven-year tenure with the NCS staff, I also directed the Technology and Programs Branch and, thus, have

been actively involved in NCS' numerous technical and engineering efforts designed to improve the resiliency and reliability of the underlying public telecommunications networks under all types of scenarios, including its work relative to the impacts of nuclear electromagnetic pulse (EMP) on telecommunications. I am honored to appear before you today to discuss the issues surrounding the vulnerabilities of our nation's critical telecommunications infrastructure to nuclear electromagnetic pulse (EMP), and to other sources of telecommunications electromagnetic disruptive effects (TEDE), and NCS' efforts to address those vulnerabilities. TEDE is a high-intensity, short-duration burst of electromagnetic energy generated by nuclear or other devices. Unless properly shielded or designed power networks or electronic devices may be damaged by this energy surge.

II. BACKGROUND ON THE NCS

A. *The NCS Mission Generally – National Security/Emergency Preparedness (NS/EP) Telecommunications*

Since the height of the Cold War, the development and maintenance of survivable national telecommunications has been an enduring national objective. The nation's telecommunications infrastructure must possess a combination of hardness, redundancy, mobility, connectivity, interoperability, restorability, and security. Over two decades ago, E.O. 12472 recognized the fundamental importance of reliable telecommunications to our national security, calling for a redundant and resilient telecommunications capable of absorbing an attack and continuing to function in support of multiple national objectives, such as connectivity for national leaders, military command and control, and continuity of government.

Similarly, in 1983, National Security Decision Directive (NSDD) No. 97 identified a survivable telecommunications infrastructure as a critical element of U.S. deterrence strategies. More

recently, Homeland Security Presidential Directive (HSPD) No. 7 recognized that, in addition to its specific national security significance, reliable telecommunications also constitutes one of the essential services that underpin American society as a whole and forms a crucial foundation for homeland security as well.

To help to achieve this objective, President Kennedy, in 1963, established the NCS "to provide necessary communications for the Federal Government under all conditions ranging from a normal situation to national emergencies and international crises, including nuclear attack." Two decades later, in 1984, President Reagan, issued E.O. 12472, which reaffirmed and expanded the membership and mission of the NCS.

In essence, the NCS is a consortium of key representatives of the Executive Office of the President (EOP) and 23 departments and agencies having national security and/or emergency preparedness (NS/EP) missions. As set forth in E.O. 12472, the NCS assists the President and the EOP in the coordination of the planning for and provision of NS/EP telecommunications for the Federal government under all circumstances, including crisis or emergency, attack, recovery, and reconstitution. E.O. 12472 charges the NCS to ensure development of a national telecommunications infrastructure that is:

- Responsive to the NS/EP needs of the President and Federal departments and agencies, including telecommunications support of national security leadership and Continuity of Government;
- Capable of satisfying priority telecommunications requirements under all circumstances through use of commercial, government, and privately owned telecommunications resources;
- Designed to incorporate the necessary combination of hardness, redundancy, mobility, connectivity, interoperability, restorability, and security to obtain the survivability of NS/EP telecommunications in all circumstances; and

- Consistent, to the maximum extent practicable, with other national telecommunications policies.

When put into place at the height of the Cold War, the larger NS/EP goal was promotion of a survivable and resilient national telecommunications infrastructure. The primary focus was on a state-based, largely monolithic threat. The fear was that a single major power would launch a first strike against military and defense industrial base targets in the United States. In the post-9/11 environment, however, the U.S. faces more asymmetric threats and the potential targets expanded to include civilian, economic, and other critical targets. This change — fundamental in terms of actors, intent, capabilities, and tactics — creates new challenges for the U.S. Government.

Such evolving and expanding threats present three basic issues for the NS/EP Telecommunications community. They (1) undermine the ability to assure the delivery of essential telecommunications services; (2) blur traditional distinctions between wartime and non-wartime functions; and (3) complicate threat assessments to the national telecommunications infrastructure.. NS/EP telecommunications were originally conceived to serve at the nexus of national security and emergency preparedness, responding to any event that has the potential for catastrophic implications for the nation. The linkage of "NS" and "EP"—and their underlying statutory authorities—enabled the US Government to organize national response efforts regardless of the threat, whether it involved a nuclear attack or a natural disaster affecting a significant region of the country. These response efforts ranged from ensuring the survival of enduring constitutional government, support to military operations, and providing federal disaster assistance. Some of these efforts are accomplished in close coordination with FEMA's Office of National Security Coordination.

In recognition of the fact that more than 95 percent of government telecommunications traffic traverses the public switched telephone network, E.O. 12472 also directed the NCS to "serve as a focal point for joint industry-government national security and emergency preparedness telecommunications planning," a principle of public-private collaboration that HSPD-7 calls for all critical infrastructure sectors.

B. *NCS Responsibilities Relative to EMP*

Part 215 of Title 47, Chapter II, of the Code of Federal Regulations (C.F.R.) establishes NCS, as the focal point within the Federal government for all EMP technical data and studies concerning telecommunications. The purposes underlying this designation were to centralize dissemination of data and the results of studies concerning the telecommunications effects of EMP and protective measures among Federal agencies and avoid duplication of research efforts.

III. NCS ACTIVITES RELATIVE TO TELECOMMUNICATIONS ELECTROMAGNETIC DISRUPTIVE EFFECTS (TEDE) FROM NUCLEAR EMP AND OTHER SOURCES

Emerging from the tactical and strategic concerns of the Cold War, analyses of potential sources of electromagnetic disruption of telecommunications services have historically focused most sharply on the effects produced by the electromagnetic pulse emanating from the detonation of a nuclear device by a hostile nation-state. For example, in a 1985 special report to the President, the National Security Telecommunications Advisory Committee (NSTAC) provided its analysis of the vulnerability of the telecommunications infrastructure to High Altitude EMP (HEMP).

Yet, while nuclear EMP remains the only mechanism to effect widespread electromagnetic disruption to telecommunications – for example, the 2004 EMP Commission notes impacts covering a geographic area 2800 km in diameter – it is important to recognize that the advance of

technology has yielded many more tools capable of producing similar telecommunications electromagnetic disruptive effects (TEDE) on a more limited, but nevertheless significant, scale. Such tools are, as a general matter, often less costly than are those necessary to create an EMP. Accordingly, consonant with its NS/EP telecommunications mission, NCS has expanded its analytical activities to encompass the full range of TEDE sources including, but not limited to, EMP.

With respect to EMP specifically, the NCS has, over the ensuing two decades since the NSTAC Report, conducted numerous studies, simulations, and tests of various elements of the telecommunications infrastructure to electromagnetic interference from a nuclear EMP. These tests, conducted in the late 1980s and into the 1990s, subjected the major telecommunications switching system components to electromagnetic radiation simulating an EMP. The information derived from these tests was used by the equipment manufacturers to implement vulnerability mitigating changes in the design of the switching systems.

Just last year, the NCS also actively participated in the congressionally-chartered *Commission to Assess the Threat from High Altitude Electromagnetic Pulse* (the "2004 EMP Commission") that examined and evaluated the state of the EMP threat at present and looking 15 years into the foreseeable future. The Commission's Report, delivered last July, concludes that EMP presents a less significant direct threat to telecommunications than it does to the National Power grid but would nevertheless disrupt or damage a functionally significant fraction of the electronic circuits in the nation's telecommunications systems in the region exposed to EMP (which could include most of the United States). The NCS concurs with this assessment.

Notably, the Commission focused on many high altitude effects from EMP, but did not delve into the threats from source region EMP, system-generated EMP, trapped radiation, and other sources of TEDE such as directed radio frequency (RF) energy weapons, which could be developed and used by terrorists against the telecommunications infrastructure. As noted above, NCS considers this to be an important area for future consideration and action. NCS' efforts relative to the potential threat posed by such other sources of TEDE fall into the following three categories:

(1) evaluating the vulnerability of the telecommunications infrastructure to the full range of electromagnetic disruptive effects;

(2) identifying measures to mitigate these effects and providing timely information to the nation on the vulnerabilities and the mitigation measures; and

(3) initiating programs that provide connectivity assurance in the event of disruption such as facility hardening and Telecommunications Services Priority (TSP) service.

As a part of its vulnerability assessment activities, the NCS participated in the congressionally-mandated "Live Fire" exercise in 2000. "Live Fire" tested military communications equipment vulnerabilities to electromagnetic disruption; however, because much of the equipment used by the military corresponds to the commercial-off-the-shelf (COTS) equipment used in the civilian telecommunications infrastructure nationally, NCS' participation in this effort facilitated tests of equipment and systems common to the Internet .

Some of our efforts have included tests, simulations and analysis to assess the vulnerability to TEDE of:

- High frequency Two-Way radio systems
- Public Service Radio Systems

- Public Telecommunications Network Switches (4E, 5E, DMS-100)
- Public Telecommunications Network Buildings and Facilities
- Satellite teleports
- Signaling, Control and Data Acquisition systems (SCADA)
- Internet edge equipments (routers, small computers)
- Internet core equipments (Switching Systems)

At present, NCS is initiating an effort to evaluate the impact of TEDE from various modalities on a large backbone router.

IV. UNDERSTANDING THE THREAT BEYOND TEDE

As noted above, the NCS is responsible for assessing all threats to the national telecommunications infrastructure. Accordingly, recognizing communication's pivotal role in deterring and/or recovering from an attack, the NCS does not look at EMP or other sources of TEDE in a vacuum, but rather in the larger context of the full range of potential threats to the telecommunications infrastructure.

In the 1980s, government and industry focused their attention on the potential destruction and damage a major first strike could generate. As the Cold War threat abated, interest turned to other potential threats, including attacks in cyberspace, weapons of mass destruction, and terrorist acts. In the dynamic threat environment of today, it remains important for industry and government to assess potential threats to the national telecommunications infrastructure. In addition to EMP and TEDE, the NCS is involved with assessing other potential vulnerabilities of the infrastructure, such as:

- Submarine Cable Landings
- Telecom hotels
- Convergence of the traditional telecommunication network with IP-based systems

Studies, modeling and simulation, and testing in these areas, as well as those involving potential EMP,, cyber, and/or physical attacks, alone or in combination with each other, will enable us to develop a fuller picture of the risk landscape as we build tools and programs to manage the risk to the nation's communications system.

Finally, as a part of the interim National Infrastructure Protection Plan (NIPP) recently released by DHS, the NCS serves as the Sector Specific Agency (SSA) for the telecommunications sector. In this lead role IAIP and NCS support and facilitate the organization of the sector to strengthen significantly the collaborative effort to identify vulnerabilities and develop mitigation strategies both within the sector as well as across sectors.

Although new, this activity is key to our ability to develop and refine cross-sector risk mitigation strategies as we work to address the risks posed by EMP and other sources of TEDE.

V. CONCLUSION

The NCS is responsible for assessing and mitigating vulnerabilities to the national telecommunications infrastructure. Accordingly, recognizing communication's pivotal role in deterring and/or recovering from an attack, the NCS has developed a vulnerability mitigation approach that is designed to address the entire spectrum of potential disruptions to the nation's telecommunications and ensure critical communications will be possible under all conditions.

The existence of EMP effects has been known since the 1940's and we have tested thoroughly our current generation of core telecommunications switches and have determined that there is minimal EMP effect on these switches. Furthermore, most of our core communications assets are in large, very well constructed facilities which provide a measure of shielding. This situation will evolve as we move to next generation networks (NGN) but we are monitoring this network evolution by testing critical components of the NGN and leveraging DoD testing.

In moving forward, the NCS has a proven history of preparing for and responding to all types of threats, founded in its ability to develop effective tools and programs combined with a trusted working relationship with industry to continually improve the hardness and survivability of the nation's communications network.

This concludes my prepared statement. I would be happy to answer any questions you may have at this time.

Attachment 1

STATEMENT OF SENATOR JON KYL
CHAIRMAN
SUBCOMMITTEE ON TERRORISM, TECHNOLOGY, AND HOMELAND SECURITY
SENATE JUDICIARY COMMITTEE

"TERRORISM AND THE EMP THREAT TO HOMELAND SECURITY"

8 MARCH 2005

Overview

Today, the Subcommittee on Terrorism, Technology, and Homeland Security will examine the threat and impact of an electromagnetic pulse (EMP) attack on the American homeland. An attack using an EMP – a phenomenon created by the detonation of a nuclear weapon – could devastate this country. The public and the Congress need to pay more attention to this danger.

Earlier this year, CIA Director Porter Goss gave chilling testimony about missing nuclear material from storage sites in Russia that may have found its way into terrorists' hands. Moreover, FBI Director Mueller confirmed new intelligence that suggest that Al Qaeda is trying to acquire and use weapons of mass destruction in some form against us.

Also, the 9/11 Commission report stated that our biggest failure was one of imagination. No one imagined that terrorists would do what they did on September 11. I want to explore new and imaginative possibilities of terrorist plots and methods. And that's why we are here today – to examine a possibility that poses a grave threat and a crippling impact to our way of life.

Last year, the EMP Commission found that EMP was one of a small number of threats that could hold our society at risk of catastrophic consequences. The effects of an EMP could potentially shock, damage, or even destroy electrical systems that fall within the striking range of a nuclear detonation. And because the United States is heavily dependent on electrical systems to provide basic services, an EMP attack has the potential to have a cascading effect on all aspects of American society.

The Commission's report found that our infrastructure – such as electrical power, telecommunications, energy, financial, transportation, emergency services, water purification and delivery, and food refrigeration – were all vulnerable to EMP attack. And in the event of an EMP attack, those infrastructures would be rendered unusable, thus inflicting widespread disruption or failure on a national scale. The death toll from such an attack is almost unthinkable. Unfortunately, the House Armed Services Committee hearing on the Commission Report occurred on the date of the release of the 9/11 Commission Report. As a result, the hearing – and the EMP Report – received virtually no coverage.

I would like to review those finding and understand the current risk we face as well as the actions we may need to take to prepare for an EMP attack.

Witnesses

The Subcommittee will hear from three highly qualified witnesses.

Dr. Lowell L. Wood, Jr.

Dr. Lowell L. Wood, Jr. is a Commissioner of the National Commission to Assess the EMP Threat to the United States; a member of the Technical Advisory Group of the U.S. Senate Select Committee on Intelligence; a member of the Undersea Warfare Experts Group of the U.S. House of Representatives Committee on Armed Services; a member of the U.S. Nuclear Strategy Forum; a Visiting Fellow at the Hoover Institution at Stanford University; and an officer and member of the Board of Directors of the Fannie and John Hertz Foundation. He is also a member of the Laboratory Director's Technical Staff, University of California Lawrence Livermore National Laboratory, where he has held numerous positions since 1972. He has received numerous awards and prizes for his work, and is the author of several hundred publications.

Dr. Peter Pry

Dr. Peter Vincent Pry was one of the CIA's chief experts on Soviet plans for EMP attack. During the Cold War, he developed much of what the U.S. government knows about Soviet planning for nuclear war; and, in the post-Cold War period, his work has been central to the U.S. government's

understanding of evolving Russian threat perceptions and military doctrine. He is the Director of the United States Nuclear Strategy Forum, a non-profit foundation established to advise Congress on the future threat environment and on the role of nuclear weapons in U.S. national security policy, and recently served on the EMP Commission staff, where he was the chief analyst on foreign views of EMP attack. Dr. Pry holds two Ph.D.s, one in history, and the other in international relations. He has authored several books on national security and military issues.

Dr. Peter Fonash, DHS, National Communications, Deputy Manager (Acting)

Dr. Peter M. Fonash is the Acting Deputy Manager, National Communications and has been a member of the Senior Executive Service since 1998. He has served in both technical and policy positions in the Federal government. Dr. Fonash earned three degrees from the University of Pennsylvania: a Bachelor of Science in electrical engineering, a Masters of Science, and a Master of Business Administration (Wharton School). He also holds a Doctor of Philosophy degree from George Mason University, School of Information Technology and Engineering. His 24 years in federal services were preceded by four years in private industry.

Conclusion

We have a distinguished panel of witnesses before us today, but I would also like to recognize the EMP Commission members who unfortunately could not be with us today. I recognize their significant contributions to help us better understand the EMP threat and what we can do about it. I would also like to recognize Senator Feinstein who also could not be with us today. I would like to thank her for all of her work and contributions as well as the great working relationship we have on this Subcommittee.

Today, I would like to look into the EMP Threat to better understand the magnitude of this threat to our civilian infrastructure, and what we may need to do to ensure we are prepared to protect our citizens, our economy, and if necessary, the means to reconstruct our nation's infrastructure.

Attachment 3

STATEMENT
DR. PETER VINCENT PRY
EMP COMMISSION STAFF
BEFORE THE
UNITED STATES SENATE
SUBCOMMITTEE ON TERRORISM, TECHNOILOGY AND HOMELAND SECURITY
March 8, 2005

FOREIGN VIEWS OF
ELECTROMAGNETIC PULSE (EMP) ATTACK

The EMP Commission sponsored a worldwide survey of foreign scientific and military literature to evaluate the knowledge, and possibly the intentions, of foreign states with respect to electromagnetic pulse (EMP) attack. The survey found that the physics of EMP phenomenon and the military potential of EMP attack are widely understood in the international community, as reflected in official and unofficial writings and statements. The survey of open sources over the past decade finds that knowledge about EMP and EMP attack is evidenced in at least Britain, France, Germany, Israel, Egypt, Taiwan, Sweden, Cuba, India, Pakistan, Iraq under Saddam Hussein, Iran, North Korea, China and Russia.

Numerous foreign governments have invested in hardening programs to provide some protection against nuclear EMP attack, indicating that this threat has broad international credibility. At least some of the new nuclear weapon states, notably India, are concerned that their military command, control, and communications may be vulnerable to EMP attack. For example, an Indian article citing the views of senior officers in the Defense Ministry (including General V. R. Raghavan) concludes: "The most complicated, costly, controversial and critically important elements of [nuclear] weaponisation are the C3I systems....Saving on a C3I system could be suicidal. With a no-first-use policy, the Indian communications systems have to be hardened to withstand the electromagnetic pulses generated by an adversarial nuclear first strike. Otherwise, no one will be fooled by the Indian nuclear deterrent." (C. Rammonohar Reddy, **The Hindu**, 1 September 1998)

Many foreign analysts perceive nuclear EMP attack as falling within the category of electronic warfare or information warfare, not nuclear warfare. Indeed, the military doctrines of at least China and Russia appear to define information warfare as embracing a spectrum ranging from computer viruses to nuclear EMP attack. For example, consider the following quote from one of China's most senior military theorists–who is credited by the PRC with inventing information warfare– appearing in his book **World War, the Third World War–Total Information Warfare**: "With their massive destructiveness, long-range nuclear weapons have combined with highly sophisticated information technology and computer technology today and warfare of the looming 21st century: information war under nuclear deterrence....Information war and traditional

Attachment 3
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." (2001)

Some foreign analysts, judging from open source statements and writings, appear to regard EMP attack as a legitimate use of nuclear weapons, because EMP would inflict no or few prompt civilian casualties. EMP attack appears to be a unique exception to the general stigma attached to nuclear employment by most of the international community in public statements. Significantly, even some analysts in Japan and Germany–nations that historically have been most condemnatory of nuclear and other weapons of mass destruction in official and unofficial forums–appear to regard EMP attack as morally defensible. For example, a June 2000 Japanese article in a scholarly journal, citing senior political and military officials, appears to regard EMP attack as a legitimate use of nuclear weapons: "Although there is little chance that the Beijing authorities would launch a nuclear attack, which would incur the disapproval of the international community and which would result in such enormous destruction that it would impede post-war cleanup and policies, a serious assault starting with the use of nuclear weapons which would not harm humans, animals, or property, would be valid. If a...nuclear warhead was detonated 40 kilometers above Taiwan, an electromagnetic wave would be propagated which would harm unprotected computers, radar, and IC circuits on the ground within a 100 kilometer radius, and the weapons and equipment which depend on the communications and electronics technology whose superiority Taiwan takes pride in would be rendered combat ineffective at one stroke...If they were detonated in the sky in the vicinity of Ilan, the effects would also extend to the waters near Yonakuni [in Okinawa], so it would be necessary for Japan, too, to take care. Those in Taiwan, having lost their advanced technology capabilities, would end up fighting with tactics and technology going back to the 19th century...They would inevitably be at a disadvantage with the PLA and its overwhelming military force superiority." (Su Tzu-yun, **Jadi**, 1 June 2000)

An article by a member of India's Institute of Defense Studies Analysis openly advocates that India be prepared to make a preemptive EMP attack, both for reasons of military necessity and on humanitarian grounds: "A study conducted in the U.S. during the late 1980s reported that a high-yield device exploded about 500 kilometers above the ground can generate an electromagnetic pulse (EMP) of the order of 50,000 volts over a radius of 2,500 kilometers around the point of burst which would be collected by any exposed conductor. Such an attack will not cause any blast or thermal effects on the ground below but it can produce a massive breakdown in the communications system....It is certain that most of the land communication networks and military command control links will be affected and it will undermine our capability to retaliate. This, in fact, is the most powerful incentive for a preemptive attack. And a high-altitude exo-atmospheric explosion may not even kill a bird on the ground." (**The Indian Express**, 17

Attachment 3
September 1999)

Although India, Pakistan, and Israel are not rogue states, they all presently have missiles and nuclear weapons giving them the capability to make EMP attacks against their regional adversaries. An EMP attack by any of these states–even if targeted at a regional adversary and not the United States–could collaterally damage U.S. forces in the region, and would pose an especially grave threat to U.S. satellites.

Many foreign analysts–particularly in Iran, North Korea, China, and Russia–view the United States as a potential aggressor that would be willing to use its entire panoply of weapons, including nuclear weapons, in a first strike. They perceive the United States as having contingency plans to make a nuclear EMP attack, and as being willing to execute those plans under a broad range of circumstances.

Russian and Chinese military scientists in open source writings describe the basic principles of nuclear weapons designed specifically to generate an enhanced-EMP effect, that they term "Super-EMP" weapons. "Super-EMP" weapons, according to these foreign open source writings, can destroy even the best protected U.S. military and civilian electronic systems.

Chinese military writings are replete with references to the dependency of United States military forces and civilian infrastructure upon sophisticated electronic systems, and to the potential vulnerability of those systems. For example, consider this quote from an official newspaper of the PLA: "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." (Zhang Shouqi and Sun Xuegui, **Jiefangjun Bao** 14 May 1996)

Russian military writings are also replete with references to the dependency of United States military forces and civilian infrastructure upon sophisticated electronic systems, and to the potential vulnerability of those systems. Indeed, Russia made a thinly veiled EMP threat against the United States on May 2, 1999. During the spring of 1999, tensions between the United States and Russia rose sharply over Operation ALLIED FORCE, the NATO bombing campaign against Yugoslavia. A bipartisan delegation from the House Armed Services Committee of the U.S. Congress met in Vienna with their Russian counterparts on the Duma International Affairs Committee, headed by Chairman Vladimir Lukin. The object of the meeting was to reduce U.S. -

Attachment 3
Russia tensions and seek Russian help in resolving the Balkans crisis. During the meeting, Chairman Lukin and Deputy Chairman Alexander Shaponov chastised the United States for military aggression in the Balkans, and warned that Russia was not helpless to oppose Operation ALLIED FORCE: "Hypothetically, if Russia really wanted to hurt the United States in retaliation for NATO's bombing of Yugoslavia, Russia could fire a submarine launched ballistic missile and detonate a single nuclear warhead at high-altitude over the United States. The resulting electromagnetic pulse would massively disrupt U.S. communications and computer systems, shutting down everything." (HASC Transcript On Vienna Conference, 2 May 1999)

Iran, though not yet a nuclear weapon state, has produced some analysis weighing the use of nuclear weapons to destroy cities, as "against Japan in World War II," compared to "information warfare" that includes "electromagnetic pulse...for the destruction of unprotected circuits." An Iranian analyst describes "terrorist information warfare" as involving not just computer viruses but attacks using "electromagnetic pulse (EMP)." (Tehran, **Siyasat-e Defa-I**, 1 March 2001)

An Iranian political-military journal, in an article entitled "Electronics To Determine Fate Of Future Wars," suggests that the key to defeating the United States is EMP attack: "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)

Iranian flight-tests of their Shahab-3 medium-range missile, that can reach Israel and U.S. forces in the Persian Gulf, have in recent years involved several explosions at high altitude, reportedly triggered by a self-destruct mechanism on the missile. The Western press has described these flight-tests as failures, because the missiles did not complete their ballistic trajectories. Iran has officially described all of these same tests as successful. The flight-tests would be successful, if Iran were practicing the execution of an EMP attack.

Iran, as noted earlier, has also successfully tested firing a missile from a vessel in the Caspian Sea. A nuclear missile concealed in the hold of a freighter would give Iran, or terrorists, the capability to perform an EMP attack against the United States homeland, without developing an ICBM, and with some prospect of remaining anonymous. Iran's Shahab-3 medium-range missile, mentioned earlier, is a mobile missile, and small enough to be transported in the hold of a freighter.

We cannot rule out that Iran, the world's leading sponsor of international terrorism, might

provide terrorists with the means to execute an EMP attack against the United States.

In closing, a few observations about the potential EMP threat from North Korea.

North Korean academic writings subscribe to the view voiced in Chinese, Russian, and Iranian writings that computers and advanced communications have inaugurated an "information age" during which the greatest strength, and greatest vulnerability, of societies will be their electronic infrastructures. According to North Korean press, Chairman Kim Chong-il is himself supposedly an avid proponent of this view. (M.A. Kim Sang-hak, "development of Information Industry and Construction of Powerful Socialist State," **Pyongyang Kyongje Yongu**, 20 May 2002)

The highest ranking official ever to defect from North Korea, Hwang Chang-yop, claimed in 1998 that North Korea has nuclear weapons and explained his defection as an attempt to prevent nuclear war. According to Hwang, in the event of war, North Korea would use nuclear weapons "to devastate Japan to prevent the United States from participating. Would it still participate, even after Japan is devastated? That is how they think." Although Hwang did not mention EMP, it is interesting that he described North Korean thinking about nuclear weapons employment as having strategic purposes–nuclear use against Japan–and not tactical purposes–nuclear employment on the battlefield in South Korea. It is also interesting that, according to Hwang, North Korea thinks it can somehow "devastate" Japan with its tiny nuclear inventory, although how precisely this is to be accomplished with one or two nuclear weapons is unknown.

Perhaps most importantly, note that the alleged purpose of a North Korean nuclear strike on Japan would be to deter the United States. At the time of Hwang's defection, in 1998, North Korea's longest-range missile then operational, the No Dong, limited North Korea's strategic reach to a strike on Japan. Today, North Korea is reportedly on the verge of achieving an ICBM capability with its Taepo Dong-2 missile, estimated to be capable of delivering a nuclear weapon to the United States.

In 2004, the EMP Commission met with very senior Russian military officers, who are experts on EMP weapons. They warned that Russian scientists had been recruited by Pyongyang to work on the North Korean nuclear weapons program. They further warned that the knowledge and technology to develop "Super-EMP" weapons had been transferred to North Korea, and that North Korea could probably develop these weapons in the near future, within a few years. The Russian officers said that the threat to global security that would be posed by a North Korea armed with "Super-EMP" weapons is unacceptable. The senior Russian military officers, who claimed to be expressing their personal views to the EMP Commission, said that, while the Kremlin could not publicly endorse U.S. preemptive action, Moscow would privately understand the strategic necessity of a preemptive strike by the United States against North Korea's nuclear complex.

This concludes my statement. Thank you for the opportunity to share this information with the U.S. Senate and the American people.

Attachment 2

OPENING STATEMENT

DR. LOWELL WOOD

ACTING CHAIRMAN,

COMMISSION TO ASSESS THE THREAT TO THE U.S. FROM ELECTROMAGNETIC PULSE ATTACK

BEFORE THE

UNITED STATES SENATE

COMMITTEE ON THE JUDICIARY

SUBCOMMITTEE ON TERRORISM, TECHNOLOGY AND HOMELAND SECURITY

HON. JON KYL, CHAIRMAN

2:30 PM, 8 MARCH 2005, 226 DIRKSEN SENATE OFFICE BUILDING

Chairman Kyl, Members of the Subcommittee, ladies and gentlemen, my fellow Commissioners and I thank you for the opportunity to testify today on the findings and recommendations of the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack, created by the Congress in Title XIV of P.L. 106-398. At the direction of the Congress, this Commission worked for two years on its statutory mandate. These efforts have included conducting actual experiments to test the potential vulnerability of modern electronics systems to EMP, and were informed by a global survey of foreign scientific and foreign military literatures to assess the knowledge, and if possible the intentions, of rogue states and other nations with respect to EMP attack. The Commission enjoyed access to all information in the possession of the Government in the course of its work, and was supported by top-quality studies and analyses on the part of many cognizant Government and contractor organizations.

The "bottom line" is that several classes of potential adversaries – including terrorist groupings – have or can acquire the capability to attack the United States with a high-altitude nuclear weapon-generated electromagnetic pulse. A determined adversary can achieve an EMP attack capability without having a high level of either military or nuclear sophistication. For example, a Scud missile launched from a freighter off the Atlantic coast of the United States could constitute a platform that would enable a terrorist group to mount an EMP attack against roughly half of the United States in population terms. Scud missiles can be purchased inexpensively (of the order of $100,000) by anyone, including private collectors, in the world's arms markets. Terrorists might buy, steal, or be given a 'no fingerprints' nuclear weapon. For example, North Korea has demonstrated willingness to sell both missiles and nuclear materials remarkably promiscuously. Iran, the world's leading sponsor of international terrorism, is widely reported to have a nuclear weapons program that is more advanced than previously suspected – and is known to have successfully test-launched a Scud missile from a vessel in the Caspian Sea, a launch mode that could be adapted, as already noted, to

Attachment 2
support an EMP attack against the United States "from the sea".

A nuclear weapon detonated at altitudes above a few dozen kilometers above the Earth's surface will generate a set of electromagnetic pulses of different types as its various outputs interact with the Earth's atmosphere. These EMPs propagate from the burst-point of the nuclear weapon to the line-of-sight on the Earth's horizon, potentially covering a vast geographic region. For example, a nuclear weapon detonated at an altitude of 400 kilometers over the central United States would cover with its primary EMP the entire continental United States, and parts of Canada and Mexico.

The immediate effects of EMP are disruption of, and damage to, electronic systems and electrical infrastructures. EMP is not reported in the scientific literature to have direct effects on people.

EMP and its effects were observed extensively during the U.S. and Soviet atmospheric test programs in 1962. During the United States STARFISH nuclear detonation – not designed or intended as a generator of EMP – at an altitude of about 400 kilometers above Johnston Island in the Pacific Ocean, some electrical systems in the Hawaiian Islands, 1,400 kilometers distant, were affected. This comparatively weak-&-distant EMP caused the failure of street-lighting systems, tripping of circuit breakers, triggering of burglar alarms, and damage to a telecommunications relay system – among other reported effects.

The Russians, in their testing that year, executed a series of high-altitude nuclear detonations above their test site in South Central Asia. They report they observed damage to both overhead and underground buried cables, some at distances of 600 kilometers. They also observed surge arrestor burnout, spark-gap breakdown, blown fuses, and failures of power supplies of various types.

What is particularly significant about EMP is that a single high-altitude nuclear detonation can produce EMP effects that can potentially disrupt or damage electronic and electrical systems over much of the United States, virtually simultaneously, at a time determined by an adversary. Thus, EMP is one of a small number of threat-types that has the potential to hold American society seriously at risk and that might result in the defeat of our military forces.

The electromagnetic field pulses produced by weapons designed and deployed with the intent to produce EMP have a high likelihood of damaging electrical power systems, electronics, and information systems upon which any reasonably advanced society – including our own – depends vitally. Their effects on systems and infrastructures dependent on electricity and electronics could be sufficiently ruinous as to qualify as catastrophic to the Nation.

Depending on the specific characteristics of the EMP attack, unprecedented cascading failures of our major infrastructures could result, in which failure of one infrastructure could 'pull down' others dependent on its functioning, and the failure of these, in turn, could seriously impede recovery of the first infrastructure-to-fail. In such events, a regional or national recovery would be long and difficult, and would seriously degrade the overall viability of our Nation and the safety, even the lives, of very large numbers of U.S. citizens.

Attachment 2

The primary avenues for EMP imposition of catastrophic damage to the Nation are through our electric power infrastructure and thence into our telecommunications, energy, and other key infrastructures. These, in turn, can seriously impact other vital aspects of our Nation's life, including the financial system; means of getting food, water, and health care to the citizenry; trade; and production of goods and services.

The recovery of any one of these key National infrastructures is dependent on others working. The longer the basic outage, the more problematic and uncertain the recovery of any of them will be. It is possible – indeed, seemingly likely -- for sufficiently-severe functional outages to become mutually reinforcing, until a point at which the degradation of the set of infrastructures could have irreversible effects on the country's ability to support any large fraction of its present human population.

EMP effects from high-altitude nuclear explosions are not new threats to our nation. The Soviet Union in the past and Russia and other nations today are capable of creating these effects. Historically, this application of nuclear weaponry was mixed with a much larger population of nuclear explosives that was the primary source of destruction, and thus EMP as a weapons effect was not the primary focus of U.S. defensive preparations. Throughout the Cold War, the United States did not try to protect its civilian infrastructure against either the physical or EMP impact of nuclear weapons, and instead depended on deterrence for whatever safety might be attained.

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

Single detonations of certain types of relatively low-yield nuclear weapons can be employed to generate potentially catastrophic EMP effects over wide geographic areas, and designs for variants of such weapons may have been illicitly trafficked for a quarter-century.

China and Russia have considered limited nuclear attack options that, unlike their Cold War plans, employ EMP as the primary or sole means of attack. Indeed, as recently as May 1999, during the NATO bombing of the former Yugoslavia, high-ranking members of the Russian Duma, meeting with a U.S. Congressional delegation to discuss the ongoing Balkans Conflict, raised the specter of a Russian EMP attack that would paralyze the United States. Open-source Chinese military writings have described, in the event of a conflict over Taiwan, using EMP as a means of defeating the U.S.

Another key difference from the past is that the U.S. has developed more than most other nations as a modern society heavily dependent on electronics, telecommunications, energy, information networks, and a rich set of financial and transportation systems that critically leverage modern technology. This asymmetry is a source of substantial economic, industrial, and societal advantages, but it creates vulnerabilities and critical interdependencies that are potentially catastrophic to the United States.

Attachment 2

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 by threatening their use – in an EMP attack. The current vulnerability of U.S. critical infrastructures can both invite and reward such attacks, if not corrected.

However, correction is feasible and well within the Nation's technical means and material resources to accomplish. Most critical infrastructure system vulnerabilities can be reduced below those levels that potentially invite attempts to create a national catastrophe. By protecting key elements in each critical infrastructure and by preparing to recover essential services, the prospects for a terrorist or rogue state being able to impose large-scale, long-term damage can be minimized. This can be accomplished reasonably and expeditiously.

Such preparation and protection can be achieved over the next several years, given a well-focused commitment by the Federal Government and a readily-affordable level of resources. We need to take actions and allocate resources to decrease the likelihood that catastrophic consequences from an EMP attack will occur, to reduce our current serious levels of vulnerability to acceptable levels and thereby reduce incentives to attack, and to remain a viable modern society, even if an EMP attack occurs. Since this is a matter of national security, the Federal Government must shoulder the responsibility of managing the most serious infrastructure vulnerabilities, including resourcing their timely obviation.

Homeland Security Presidential Directives 7 and 8 lay the authoritative basis for the Federal Government to act vigorously and coherently to mitigate many of the risks to the Nation from terrorist attack. The effects of EMP on our major civilian infrastructures lie within these directives, and the directives specify adequate responsibilities and provide sufficient authorities to deal with the civilian sector consequences of an EMP attack.

In particular, the Department of Homeland Security has been established, led by a Secretary with authority, responsibility, and the obligation to request needed resources for the mission of protecting the U.S. and recovering from the impacts of the most serious threats. This official must assure that plans, resources, and implementing structures are in place to accomplish these objectives, specifically with respect to the EMP threat. In doing so, DHS must work in conjunction with the other governmental institutions and with experts in the private sector to efficiently accomplish this mission. It is important that metrics for assessing improvements in prevention, protection, and recovery be put in place and then evaluated -- and that progress be reported regularly and independently reviewed.

Specific recommendations are provided in the EMP Commission's report with respect to both the particulars for securing each of the most critical National infrastructures against EMP threats and the governing principles for addressing these issues of national survival and recovery in the aftermath of an EMP attack. Much of the problem can be addressed very economically, without major capital investments, but by developing effective plans to meet the challenges posed by EMP threats. For example, one major Commission finding is that the electric power grid is the "keystone" infrastructure,

upon which all other infrastructures depend. Yet today, there is no plan for "black-starting" the power grid in the event of a Nation-wide collapse of the system. If the electric power grid can be quickly recovered, the other infrastructures can also be recovered adequately in the aftermath of an EMP attack. Making the key aspects of the Nation's infrastructures more robust against EMP attack will also pay dividends in protecting against other types of large-scale problems with them, such as natural disasters.

This concludes my statement. Again, my colleagues and I thank you for the opportunity to report the findings and recommendations of the EMP Commission to the United States Senate.