Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack

Volume 1: Executive Report
2004

Dr. John S. Foster, Jr.
Mr. Earl Gjelde
Dr. William R. Graham (Chairman)
Dr. Robert J. Hermann
Mr. Henry (Hank) M. Kluepfel
GEN Richard L. Lawson, USAF (Ret.)
Dr. Gordon K. Soper
Dr. Lowell L. Wood, Jr.
Dr. Joan B. Woodard

CHARTER

Public Law 106-398, Title XIV

SEC. 1402. DUTIES OF COMMISSION

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

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

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

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

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

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

The findings and recommendations presented in this report are the independent judgments of this Commission and should not be attributed to any other people or organizations. This report presents the unanimous views of the Commissioners.

ABSTRACT

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

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

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

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

CONTENTS

APPENDIXES

FIGURES

OVERVIEW

EMP IS CAPABLE OF CAUSING CATASTROPHE FOR THE NATION

The high-altitude nuclear weapon-generated electromagnetic pulse (EMP) is one of a small number of threats that has the potential to hold our society seriously at risk and might result in defeat of our military forces.

Briefly, a single nuclear weapon exploded at high altitude above the United States will interact with the Earth's atmosphere, ionosphere, and magnetic field to produce an electromagnetic pulse (EMP) radiating down to the Earth and additionally create electrical currents in the Earth. EMP effects are both direct and indirect. The former are due to electromagnetic "shocking" of electronics and stressing of electrical systems, and the latter arise from the damage that "shocked"—upset, damaged, and destroyed—electronics controls then inflict on the systems in which they are embedded. The indirect effects can be even more severe than the direct effects.

The damage level could be sufficient to be catastrophic to the Nation, and our current vulnerability invites attack.

The electromagnetic fields 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 American society depends. Their effects on dependent systems and infrastructures could be sufficient to qualify as catastrophic to the Nation.

Depending on the specific characteristics of the attacks, unprecedented cascading failures of our major infrastructures could result. In that event, a regional or national recovery would be long and difficult and would seriously degrade the safety and overall viability of our Nation. The primary avenues for catastrophic damage to the Nation are through our electric power infrastructure and thence into our telecommunications, energy, and other infrastructures. These, in turn, can seriously impact other important aspects of our Nation's life, including the financial system; means of getting food, water, and medical care to the citizenry; trade; and production of goods and services. The recovery of any one of the key national infrastructures is dependent on the recovery of others. The longer the outage, the more problematic and uncertain the recovery will be. It is possible

for the functional outages to become mutually reinforcing until at some point the degradation of infrastructure could have irreversible effects on the country's ability to support its population.

EMP effects from nuclear bursts are not new threats to our nation. The Soviet Union in the past and Russia and other nations today are potentially capable of creating these effects. Historically, this application of nuclear weaponry was mixed with a much larger population of nuclear devices that were the primary source of destruction, and thus EMP as a weapons effect was not the primary focus. 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 its safety.

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 US without regard for their own safety. 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.

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 US congressional delegation to discuss the Balkans conflict, raised the specter of a Russian EMP attack that would paralyze the United States.

Another key difference from the past is that the US 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 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 disastrous to the United States. Therefore, terrorists or state actors that possess relatively unsophisticated missiles armed with nuclear weapons may well calculate that, instead of destroying a city or military base, they may obtain the greatest political-military utility from one or a few such weapons by using them—or threatening their use—in an EMP attack. The current vulnerability of US

critical infrastructures can both invite and reward attack if not corrected; however, correction is feasible and well within the Nation's means and resources to accomplish.

WE CAN PREVENT AN EMP CATASTROPHE

The Nation's vulnerability to EMP that gives rise to potentially large-scale, long-term consequences can be reasonably and readily reduced below the level of a potentially catastrophic national problem by coordinated and focused effort between the private and public sectors of our country. The cost for such improved security in the next 3 to 5 years is modest by any standard—and extremely so in relation to both the war on terror and the value of the national infrastructures involved. The appropriate response to this threatening situation is a balance of prevention, protection, planning, and preparations for recovery. Such actions are both rational and feasible. A number of these actions also reduce vulnerabilities to other serious threats to our infrastructures, thus giving multiple benefits.

NATURE OF THE EMP THREAT

High-altitude EMP results from the detonation of a nuclear warhead at altitudes of about 40 to 400 kilometers above the Earth's surface. The immediate effects of EMP are disruption of, and damage to, electronic systems and electrical infrastructure. EMP is not reported in the scientific literature to have direct effects on people in the parameter range of present interest.

EMP and its effects were observed during the US and Soviet atmospheric test programs in 1962. Figure 1 depicts the 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 electronic and electrical systems in the Hawaiian Islands, 1400 kilometers distant, were affected, causing the failure of street-lighting systems, tripping of circuit breakers, triggering of burglar alarms, and damage to a telecommunications relay facility. In their testing that year, the Soviets executed a series of nuclear detonations in which they exploded 300 kiloton weapons at approximately 300, 150, and 60 kilometers above their test site in South Central Asia. They report that on each shot they observed damage to overhead and underground buried cables at distances of 600 kilometers. They also observed surge arrestor burnout, spark-gap breakdown, blown fuses, and power supply breakdowns.

What is significant about an EMP attack is that one or a few high-altitude nuclear detonations 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.

Widespread red air glow (6300 å) amid dark clouds, caused mostly by x-ray-excited atomic oxygen (i.e., oxygen by photoelectrons liberated by Starfish X-rays)

Figure 1. Starfish Nuclear Detonation

Gamma rays from a high-altitude nuclear detonation interact with the atmosphere to produce a radio-frequency wave of unique, spatially varying intensity that covers everything within line-of-sight of the explosion's center point. It is useful to focus on three major EMP components.

FIRST EMP COMPONENT (E1)

The first component is a free-field energy pulse with a rise-time measured in the range of a fraction of a billionth to a few billionths of a second. It is the "electromagnetic shock" that disrupts or damages electronics-based control systems, sensors, communication systems, protective systems, computers, and similar devices. Its damage or functional disruption occurs essentially simultaneously over a very large area, as illustrated in Figure 2.

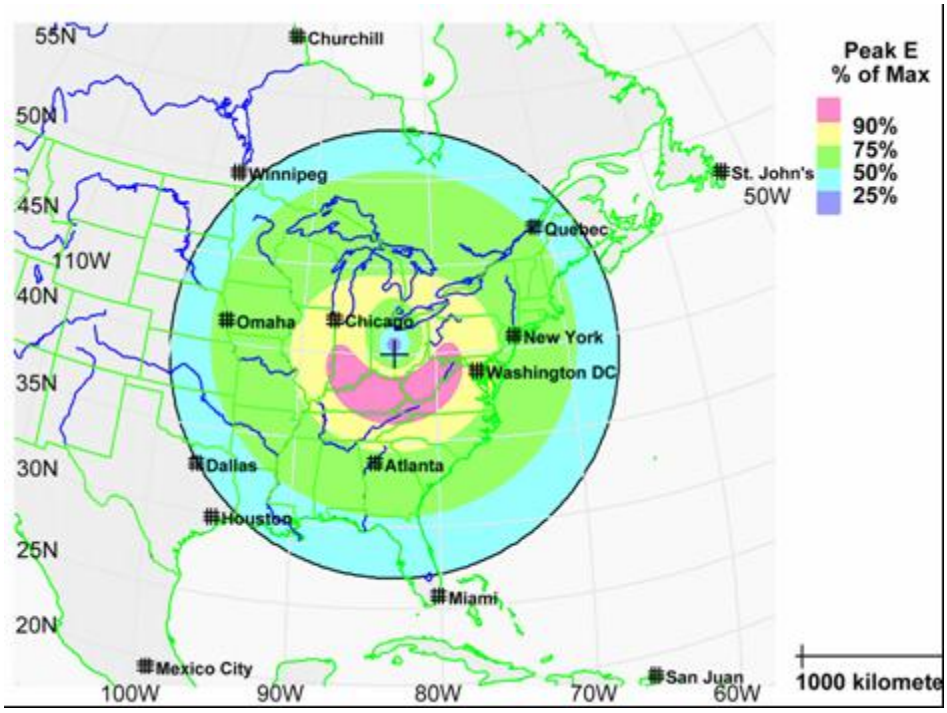


Figure 2. Illustrative EMP Effects – Fast Pulse

SECOND EMP COMPONENT (E2

The middle-time component covers roughly the same geographic area as the first component and is similar to lightning in its time-dependence, but is far more geographically widespread in its character and somewhat lower in amplitude. In general, it would not be an issue for critical infrastructure systems since they have existing protective measures for defense against occasional lightning strikes. The most significant risk is synergistic, because the E2 component follows a small fraction of a second after the first component's insult, which has the ability to impair or destroy many protective and control features. The energy associated with the second component thus may be allowed to pass into and damage systems.

THIRD EMP COMPONENT (E3)

The final major component of EMP is a subsequent, slower-rising, longer-duration pulse that creates disruptive currents in long electricity transmission lines, resulting in damage to electrical supply and distribution systems connected to such lines (Figure 3). The sequence of E1, E2, and then E3 components of EMP is important because each can cause damage, and the later damage can be increased as a result of the earlier damage. In the example depicted in Figures 2 and 3, about 70% of the total electrical power load of the United States is within the region exposed to the EMP event.

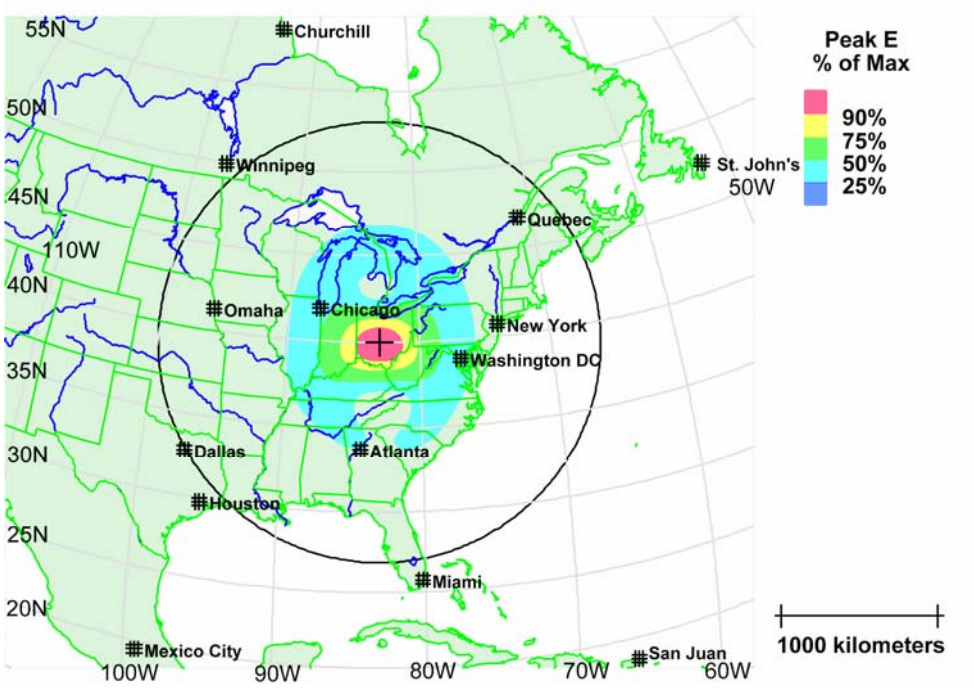


Figure 3. Illustrative EMP Effects – Slow Pulse Protection and Recovery of Civilian Infrastructures

PREVENTION

An EMP attack is one way for a terrorist activity to use a small amount of nuclear weaponry—potentially just one weapon—in an effort to produce a catastrophic impact on our society, but it is not the only way. In addition, there are potential applications of surface-burst nuclear weaponry, biological and chemical warfare agents, and cyber attacks that might cause damage that could reach large-scale, long-term levels. The first order of business is to prevent any of these attacks from occurring.

The US must establish a global environment that will profoundly discourage such attacks. We must persuade nations to forgo obtaining nuclear weapons or to provide acceptable assurance that these weapons will neither threaten the vital interests of the United States nor fall into threatening hands.

For all others, we must make it difficult and dangerous to acquire the materials to make a nuclear weapon and the means to deliver them. We must hold at risk of capture or destruction anyone who has such weaponry, wherever they are in the world.

The first order of business is to prevent any of these attacks from occurring.

Those who engage in or support these activities must be made to understand that they do so at the risk of everything they value. Those who harbor or help those who conspire to create these weapons must suffer serious consequences as well.

In case these measures do not completely succeed, we must have vigorous interdiction and interception efforts to thwart delivery of all such weaponry. To support this strategy, the US must have intelligence capabilities sufficient to understand what is happening at each stage of developing threats. In summary, the costs of mounting such attacks must be made to be great in all respects, and the likelihood of successful attack rendered unattractively small.

The current national strategy for war on terrorism already contains all of these elements. The threat of an EMP attack further raises what may be at stake.

To further forestall an EMP attack, we must reduce our vulnerability to EMP and develop our ability to recover, should there be an attack, in order to reduce the incentives to use such weaponry. We should never allow terrorists or rogue states a "cheap shot" that has such a large and potentially devastating impact.

Protection and Recovery of Civilian Infrastructures

Each critical infrastructure in the US is dependent upon other infrastructures (Figure 4). The interdependence on the proper functioning of such systems constitutes a hazard when threat of widespread failures exists. The strong interdependence of our critical national infrastructures may cause unprecedented challenges in attempts to recover from the widespread disruption and damage that would be caused by an EMP attack.

All of the critical functions of US society and related infrastructures—electric power, telecommunications, energy, financial, transportation, emergency services, water, food, etc.—have electronic devices embedded in most aspects of their systems, often providing critical controls. Electric power has thus emerged as an essential service underlying US society and all of its other critical infrastructures. Telecommunications has grown to a critical level but may not rise to the same level as electrical power in terms of risk to the Nation's survival. All other infrastructures and critical functions are dependent upon the support of electric power and telecommunications. Therefore, we must make special efforts to prepare and protect these two high-leverage systems.

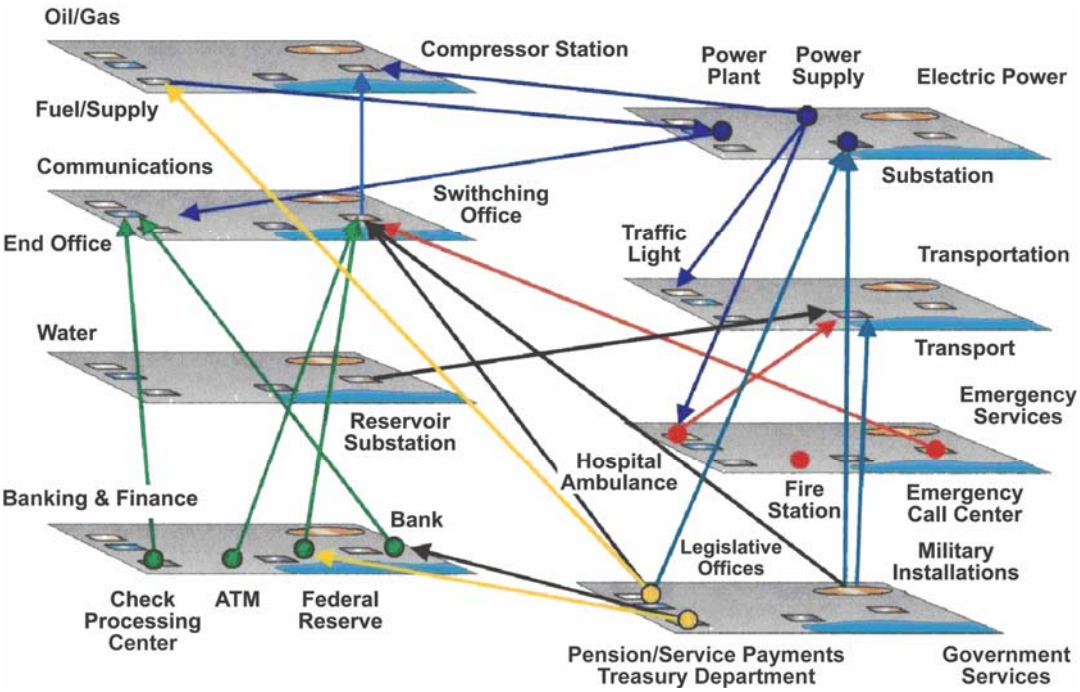


Figure 4. Interdependent Infrastructure Sectors

Most critical infrastructure system vulnerabilities can be reduced below the level that potentially invites 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 achieve 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 few years, given a dedicated commitment by the federal government and an affordable investment 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 level 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.

The most critical infrastructure system vulnerabilities can be reduced below those levels that invite attack or cause a national catastrophe.

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 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 (DHS) has been established, led by a Secretary with authority, responsibility, and the obligation to request needed resources for the mission of protecting the US 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 established governmental institutions and with experts in the private sector to most 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. DHS must clearly and expeditiously delineate its responsibility and actions in relation to other governmental institutions and the private sector, in order to provide clear accountability and avoid confusion and duplication of effort.

Specific recommendations are provided below 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 EMP attack.

STRATEGY AND RECOMMENDATIONS

It will not be possible to reduce the incentives for an EMP attack to an acceptable level of risk through defensive protection measures alone. It is possible to achieve an acceptable level of risk and reduced invitation to an EMP attack with a strategy of:

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

The cost for such improved security in the next 3 to 5 years is modest by any standard—and extremely so in relation to both the war on terror and the value of the national infrastructures involved. Costs at later times may be adjusted to deal with the then-apparent threat and future levels of effort required.

INTELLIGENCE, INTERDICTION, AND DETERRENCE

The federal government's efforts to establish and maintain a global environment that profoundly discourages potentially catastrophic attacks is our first line of defense. The development, trading, and movement of critical materials and weapons useful for mounting WMD attacks, including those that are based on the use of EMP, must be identified as early in the process as possible. The methods and materials that could encourage an EMP attack must be added to the list of threats presently being sought out and annihilated. The US and its allies against transnational terrorism must make it

exceedingly difficult and dangerous for organizations to position themselves to be a threat, or allow others to use their country and its assets in order to become a threat, specifically including EMP threats. We must hold potential perpetrators at risk of capture or destruction, whenever and wherever in the world they operate.

Protecting Critical Components of the Infrastructure

Some components of critical infrastructures, such as large turbines, generators, and high-voltage transformers in electrical power systems, and electronic switching systems in telecommunication systems, would require long periods of time to repair or replace. These components should be configured so that even under electronic disruption and damage, such as could be produced by EMP, they do not become further damaged in the course of shutting down or attempting to restore themselves. This type of damage has occurred in the past. During the Northeast power blackout of 1965, Consolidated Edison generators, transformers, motors, and auxiliary equipment were damaged by the sudden shutdown. In particular, the #3 unit at the Ravenswood power plant in New York City suffered damage when the blackout caused loss of oil pressure to the main turbine bearing. The damage kept that unit out of service for nearly a year, and more immediately, complicated and delayed the restoration of service to New York City.

Maintaining the Capability to Monitor and Evaluate the Condition of Critical Infrastructures

After an EMP attack, system operators and others in positions of authority and responsibility must have immediate access to information sufficient to characterize the state of their critical infrastructure systems. Without such system monitoring and reporting information, the system operators will not have the information required to evaluate the extent of the loss of infrastructure and know how to begin restoration of their systems. They may even induce further damage by taking inappropriate actions or failing to take necessary actions. During the time leading up to the August 14, 2003, Midwest power blackout that affected both the United States and Canada, key system operators did not have a functioning alarm system, did not recognize that the alarm system was not functioning, and had only fragmentary information on the changing configuration of the rapidly collapsing power grid for which they were responsible.

Recognizing EMP Attack

Electronic upsets and failures occur under normal operating circumstances, even in high-reliability equipment such as that supporting critical infrastructure. EMP-induced

upsets and failures, however, are different from those encountered in the normal operation of infrastructure systems, and in fact have unique aspects not encountered under any other circumstances.

EMP produces nearly simultaneous upset and damage of electronic and of other electrical equipment over wide geographic areas, determined by the altitude, character, and explosive yield of the EMP-producing nuclear explosion. Since such upset and damage is not encountered in other circumstances and particularly not remotely to the same scale, the normal experience of otherwise skilled system operators and others in positions of responsibility and authority will not have prepared them to identify what has happened to the system, what actions to take to minimize further adverse consequences, and what actions must be carried out to restore the impacted systems as swiftly and effectively as possible.

Special system capabilities and operator awareness, planning, training, and testing will be required to deal with EMP-induced system impacts. The first requirement is for the operators of critical infrastructure systems to be able to determine that a high-altitude nuclear explosion has occurred and has produced a unique set of adverse effects on their systems. That information can be provided by local electromagnetic sensors, by information from Earth satellite systems, or by other means. Whatever the means, the operators and others in positions of authority and responsibility must receive the information immediately. Therefore, the EMP event notification system must itself be highly reliable during and after an EMP attack.

Operators and others in positions of authority and responsibility must be trained to recognize that an EMP attack in fact has taken place, to understand the wide range of effects it can produce, to analyze the status of their infrastructure systems, to avoid further system degradation, to dispatch resources to begin effective system restoration, and to sustain the most critical functions while the system is being repaired and restored. Failures similar to those induced by EMP do not occur in normal system operation; therefore, the training for, and experience developed in the course of, normal system operation will not provide operators with the skills and knowledge base necessary to perform effectively after EMP-induced system disruption and failure. Training, procedures, simulations, and exercises must be developed and carried out that are specifically designed to contend with EMP-induced effects.

Planning to Carry Out a Systematic Recovery of Critical Infrastructures

A crisis such as the immediate aftermath of an EMP attack is not the time to begin planning for an effective response. Plans to avoid causing further damage to critical infrastructures and to carry out a systematic recovery of those infrastructures must be in hand at the earliest possible time. Planning for responding to an EMP attack should begin now and should be carried out jointly by system operators, hardware and software providers, and experts in both the government and private sectors.

Individual infrastructure systems have many similar electronically based control and monitoring functions. The primary features of EMP attack mitigation in each infrastructure include elements of protection of critical functions, identifying where damage within the system is located, dispatch/allocation of resources to allow for timely restoration and development of operational procedures including simulation of both individual and interacting infrastructures, training, testing, and governance. This requires test and evaluation of both existing and future systems to identify weak spots subject to EMP damage and focus mitigation activities accordingly. EMP protection thus has a substantial aspect focused on individual functioning units within each system that contains electronic components, although not necessarily on the individual electronic subcomponents of these units themselves. These units include distributed Supervisory Control and Data Acquisition (SCADA) modules, mobile communicators, radios, embedded control computers, etc. New units can be EMP-hardened for a very small fraction of the cost of the non-hardened item, e.g., 1% to 3% of cost, if hardening is done at the time the unit is designed and manufactured. In contrast, retrofitting existing functional components is potentially an order of magnitude more expensive and should be done only for critical system units. It is important to note, however, that for protection to remain functional, it must be tested and maintained in its operational mode with rigor and discipline.

Training, Evaluating, Red Teaming, and Periodically Reporting to the Congress

Identifying an EMP attack, understanding the state of the system after attack, developing and implementing plans for system restoration, and having operators and others in positions of authority and responsibility trained to recognize and respond effectively are elements of strategy that are common to managing the effects of EMP for each of the Nation's critical infrastructure components. Conducting and evaluating the results of training, simulations, tests, and Red Team activities, and periodically reporting

the results to senior executive branch leaders, the Congress, and the public are important elements of being well-prepared for EMP attack, which in turn will sharply reduce the incentives for conduct of such an attack.

Defining the Federal Government's Responsibility and Authority to Act

Governance of the critical infrastructures such as electrical power systems and communications is presently distributed among statutory governmental entities at the federal, state, regional, and municipal levels, as well as among a variety of non-governmental entities. A multiplicity of statutory bodies, private companies, associations, and individual owners also participate in determining decisions and actions. Nevertheless, the process is coordinated, albeit loosely, to produce normal efficient, reliable, and high quality service that is the envy of the world—in a peacetime environment.

A terrorist threat—let alone a terrorist attack—is outside the ambit of normal governance of the key national infrastructures. In dealing with such threats, the Department of Homeland Security has the unique and sole responsibility and authority to govern the specific actions and involved parties within the US, including requesting enabling Congressional funding as appropriate and necessary. DHS must interact with other governmental institutions and the private sector in defining liability, responsibility and funding in order to enable private and government facilities, such as independent power plants, to contribute their capability in a time of national need, yet not interfere with market creation and operation to the maximum extent practical.

DHS must interact with other governmental institutions and the private sector in defining liability, responsibility, and funding in order to enable private and government facilities, such as independent power plants, to contribute their capability in a time of national need, yet not interfere with market creation and operation to the maximum extent practical.

Industry associations, system owners/providers, private consultants, and universities all will be able to contribute useful levels of knowledge and skills. DHS is responsible for making the prudent trade-offs within each mitigation activity between performance, risk, schedule, and cost in relation to consequent system protection and then-expected risk in order to achieve maximum protection. For example, some actions taken to protect a system from an EMP attack may diminish the reliability or quality of that system's normal commercial performance, while other actions may improve the performance.

As an example of resources readily available to DHS with respect to the electric system, the North American Reliability Counsel (NERC) and the Electric Power Research Institute are well-positioned to provide much of the support needed in regard to the EMP threat. Working closely with industry and these institutions, the DHS should provide for the necessary capability to control the national bulk electricity supply system in order to protect critical services, minimize its self-destruction in the event of an EMP attack, and recover its normal capabilities as rapidly and effectively as possible thereafter.

Recognizing the Opportunities for Shared Benefits

Most of the following initiatives and actions the Commission recommends militate against more than an EMP attack. The protection and/or rapid restoration of critical infrastructures in the civilian sector from an EMP attack also will be effective against other types of infrastructure disruptions, such as attacks aimed at directly damaging or destroying key components of the electrical system, and natural or accidental large-scale disruptions are also significantly mitigated by these same initiatives. Some of these steps also enhance reliability and quality of critical infrastructures, which is a major direct benefit to the US economy and to our way of life.

Conducting Research and Development

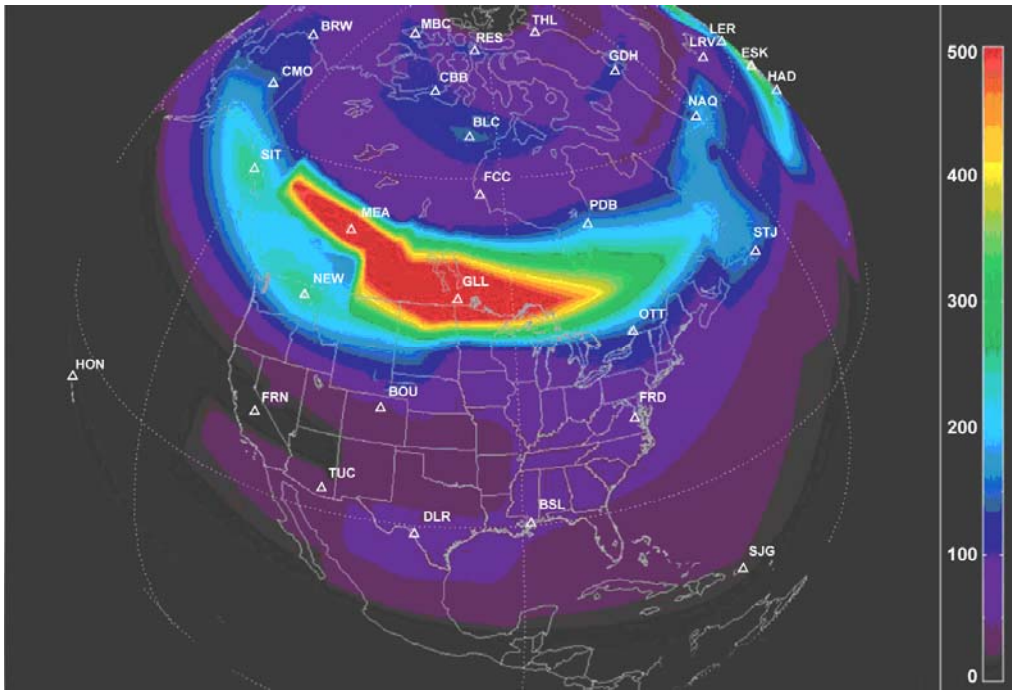
Very little research and development addressing EMP-related system response protection and recovery issues has been done for more than a decade. Conducting research to better understand infrastructure system effects and developing cost-effective solutions to manage these effects will be important to understanding the implications of the rapid evolution of electronics and electrical systems, and their growing role in controlling and operating modern critical infrastructure.

ELECTRIC POWER INFRASTRUCTURE

NATURE OF THE PROBLEM

Electric power is integral to the functioning of electronic components. For highly reliable systems such as commercial and military telecommunications, electric power usually comes from batteries (in the short term), local emergency power supplies (generally over time-intervals of less then 72 hours), and electricity delivered through the local electrical utility ("power" lines in the home, office and factory). Local emergency power supplies are limited by supplies of stored fuel. Increasingly, locally stored fuel in buildings and cities is being reduced for fire safety and environmental pollution reasons, so that the emergency generation availability without refueling is limited.

Geomagnetic storms, a natural phenomenon driven by the solar wind, may, by a different physical mechanism, produce ground-induced currents (GIC) that can affect the electrical system in a manner similar to the E3 component of EMP. Disruptions caused by geomagnetic storms, such as the collapse of Quebec Hydro grid during the geomagnetic storm of 1989, have occurred many times in the past (Figure 5).



Geomagnetic field disturbance conditions, dB/dt (nT/min) over North America at time 7:45 UT on March 13, 1989

Source: Metatech Corporation, Applied Power Solutions

Figure 5. Extent of 1989 Geomagnetic Storm

Depending on the explosive yield of the nuclear weapon used, EMP-induced GIC may be several times larger than that produced by the average geomagnetic storm, and may even be comparable to those expected to arise in the largest geomagnetic storm ever observed. It may also occur over an area not normally affected by historic geomagnetic storms.

The North American economy and the functioning of the society as a whole are critically dependent on the availability of electricity, as needed, where and when needed. The electric power system in the US and interconnected areas of Canada and Mexico is outstanding in terms of its ability to meet load demands with high quality and reliable electricity at reasonable cost. However, over the last decade or two, there has been relatively little large-capacity electric transmission constructed and the generation additions that have been made, while barely adequate, have been increasingly located considerable distances from load for environmental, political, and economic reasons. As a result, the existing National electrical system not infrequently operates at or very near local limits on its physical capacity to move power from generation to load. Therefore, the slightest insult or upset to the system can cause functional collapse affecting significant numbers of people, businesses, and manufacturing. It is not surprising that a single EMP attack may well encompass and degrade at least 70% of the Nation's electrical service, all in one instant.

The impact of such EMP is different and far more catastrophic than that effected by historic blackouts, in three primary respects:

1. The EMP impact is virtually instantaneous and occurs simultaneously over a much larger geographic area. Generally, there are neither precursors nor warning, and no opportunity for human-initiated protective action. The early-time EMP component is the "electromagnetic shock" that disrupts or damages electronics-based control systems and sensors, communication systems, protective systems, and control computers, all of which are used to control and bring electricity from generation sites to customer loads in the quantity and quality needed. The E1 pulse also causes some insulator flashovers in the lower-voltage electricity distribution systems (those found in suburban neighborhoods, in rural areas and inside cities), resulting in immediate broad-scale loss-of-load. Functional collapse of the power system is almost definite over the entire affected region, and may cascade into adjacent geographic areas.
2. The middle-time EMP component is similar to lightning in its time-dependence but is far more widespread in its character although of lower amplitude—essentially a great many lightning-type insults over a large geographic area which might obviate protection. The late-time EMP component couples very efficiently

to long electrical transmission lines and forces large direct electrical currents to flow in them, although they are designed to carry only alternating currents. The energy levels thereby concentrated at the ends of these long lines can become large enough to damage major electrical power system components. The most significant risk is synergistic, because the middle and late-time pulses follow after the early-time pulse, which can impair or destroy protective and control features of the power grid. Then the energies associated with the middle and late-time EMP thus may pass into major system components and damage them. It may also pass electrical surges or fault currents into the loads connected to the system, creating damage in national assets that are not normally considered part of the infrastructure per se. Net result is recovery times of months to years, instead of days to weeks.

3. Proper functioning of the electrical power system requires communication systems, financial systems, transportation systems, and—for much of the generation—continuous or nearly continuous supply of various fuels. However, the fuel-supply, communications, transportation, and financial infrastructures would be simultaneously disabled or degraded in an EMP attack and are dependent upon electricity for proper functioning. For electrical system recovery and restoration of service, the availability of these other infrastructures is essential. The longer the outage, the more problematic, and uncertainty-fraught the recovery will be.

The recent cascading outage of August 14, 2003, is an example of a single failure compounded by system weaknesses and human mistakes. It also provides an example of the effectiveness of protective equipment. However, with EMP there are multiple insults coupled with the disabling of protective devices simultaneously over an extremely broad region—damage to the system is likely and recovery slow.

Recommended Mitigation and Responsibility

The electrical system is designed to break into "islands" of roughly matching generation and load when a portion of the system receives a severe electrical insult. This serves both to protect electricity supply in the non-impacted regions and to allow for the stable island-systems to be used to "restart" the island(s) that have lost functionality. With EMP, the magnitude, speed, and multi-faceted nature of the insult, its broad geographic reach, along with the number of simultaneous insults, and the adverse synergies all are likely to result in a situation where the islanding scheme will fail to perform as effectively as intended, if at all. Since the impacted geographic area is large, restoring the system from the still-functioning perimeter regions would take a great deal of time, possibly weeks to months at best. Indeed, the only practical way to restart much of the impacted electrical system may be with generation that can be started without an external power source. This is called "black start" generation and primarily includes

hydroelectric (including pumped storage), geothermal, and independent diesel generators of modest capacity.

The recommended actions will substantially improve service and recovery during "normal" large-scale blackouts, and will critically enable recovery under EMP circumstances.

PROTECTION

It is impractical to protect the entire electrical power system from damage by an EMP attack. There are too many components of too many different types, manufacturers, designs, and vulnerabilities within too many jurisdictional entities, and the cost to retrofit is too great. Widespread functional collapse of the electrical power system in the area affected by EMP is possible in the face of a geographically broad EMP attack, with even a relatively few unprotected components in place. However, it is practical to reduce to low levels the probability of widespread damage to major power system components that require long times to replace. This will enable significantly improved recovery times, since it avoids the loss of long lead-time and critical components. It is important to protect the ability of the system to fragment gracefully into islands, to the extent practical in the particular EMP circumstance. This approach is cost-efficient and can leverage efforts to improve reliability of bulk electricity supply and enhance its security against the broader range of threats.

Widespread functional collapse of the electric power system in the area affected by EMP is likely.

RESTORATION

The key to minimizing adverse effects from loss of electrical power is the speed of restoration. Restoration involves matching generation capacity to a load of equivalent size over a transmission network that is initially isolated from the broader system. The larger system is then functionally rebuilt by bringing that mini system, or "island," to the standard operating frequency and thereupon by adding more blocks of generation and load to this core in amounts that can be absorbed by the growing subsystem. This is a demanding and time-consuming process in the best of circumstances. In the singular circumstance of an EMP attack with multiple damaged components, related infrastructure failures, and particularly severe challenges in communications and transportation, the time required to restore electrical power is expected to be considerably longer than we have experienced in recent history.

However, by protecting key system components needed for restoration, by structuring the network to fail gracefully, and by creating a comprehensive prioritized recovery plan for the most critical power needs, the risk of an EMP attack having a catastrophic effect on the Nation can be greatly reduced. DHS must ensure that the mitigation plan is jointly developed by the federal government and the electric power industry, implemented fully, instilled into systems operations, and tested and practiced regularly to maintain a capability to respond effectively in emergencies. The North American Reliability Council and the Electric Power Research Institute are aptly positioned to provide much of what's needed to support DHS in carrying out its responsibilities. The US Energy Association is well-suited to coordinating activities between and among the various energy sectors that together affect the electric power system and its vitality.

ESSENTIAL COMPONENT PROTECTION

1. Assure protection of high-value long-lead-time transmission assets.
2. Assure protection of high-value generation assets. System-level protection assurance is more complex due to the need for multiple systems to function in proper sequence.
3. Assure Key Generation Capability. Not all plants can or should be protected. However, regional evaluation of key generating resources necessary for recovery should be selected and protected.
    a. Coal-fired generation plants make up nearly half the Nation's generation and are generally the most robust overall to EMP, with many electromechanical controls still in operation. Such coal plants also normally have at least a few days to a month of on-site fuel storage.
    b. Natural gas-fired combustion turbines and associated steam secondary systems represent the newest and a significant contributor to meeting loads. These have modern electronics-based control and thus are more vulnerable. Natural gas is not stored on-site and likely will be interrupted in an EMP attack. However, provision can be made to have gas-fired plants also operate on fuel oil; many do already.
    c. Nuclear plants produce roughly 20% of the Nation's generation and have many redundant fail-safe systems that tend to remove them from service whenever any system upset is sensed. Their safe shut down should be assured, but they will be unavailable until near the end of restoration.
    d. Hydroelectric power is generally quite robust to EMP, and constitutes a substantial fraction of total national generation capacity, albeit unevenly distributed geographically.

e. In general, the various distributed and renewable fueled generators are not significant enough at this time to warrant special protection.

f. Black start generation of all types is critical and will need to be protected from EMP upset or damage.

4. Assure functional integrity of critical communications channels. The most critical communications channels in the power grid are the ones that enable recovery from collapse, such as ones that enable manual operation and coordination-supporting contacts between distant system operators and those that support system diagnostics. Generation, switching, and load dispatch communications support is next in importance.
5. Assure availability of emergency power at critical facilities needed for restoration. Transmission substations need uninterruptible power to support rapid restoration of grid connectivity and operability, and thereby to more quickly restore service. Most have short-life battery backup systems, but relatively few have longer-duration emergency generators; much more emphasis on the latter is needed.
6. Assure protection of fuel production and its delivery for generation. Fuel supply adequate to maintain critical electrical service and to restore expanded service is critical. See Fuel/Energy Infrastructure, page 35) for details.
7. Expand and assure intelligent islanding capability. The ability of the larger electrical power system to break into relatively small subsystem islands is important to mitigate overall EMP impacts and provide faster restoration.
8. Develop and deploy system test standards and equipment. Device-level robustness standards and test equipment exist, but protection at the system level is the overarching goal. System-level robustness improvements such as isolators, line protection, and grounding improvements will be the most practical and least expensive in most cases relative to replacement with more robust individual component devices. Periodic testing of system response is necessary.

System Restoration

1. Develop and enable a restoration plan. This plan must prioritize the rapid restoration of power to government-identified critical service. Sufficient black start generation capacity must be provided where it is needed in the associated subsystem islands, along with transmission system paths that can be isolated and connected to matching loads. The plan must address outages with wide geographic coverage, multiple major component failures, poor communication capabilities, and widespread failure of islanding schemes within the EMP-affected area. Government and industry responsibilities must be unequivocally and completely assigned. All necessary legal and financial arrangements, e.g., for indemnification, must be put into place to allow industry to implement specified government priorities with respect to service restoration, as well as to deal with potential environmental and technical hazards in order to assure rapid recovery.

2. Simulate, train, exercise, and test the plan. Simulators must be developed for use in training and developing procedures similar to those in the airline industry; a handful should suffice for the entire country. Along with simulation and field exercises, Red Team discipline should be employed to surface weaknesses and prioritize their rectification.
3. Assure sufficient numbers of adequately trained recovery personnel.
4. Assure availability of replacement equipment. R&D is under way—and should be vigorously pursued—into the production of emergency "universal" replacements. The emergency nature of such devices would trade efficiency and service-life for modularity, transportability, and affordability.
5. Implement redundant backup diagnostics and communication. Assure that system operators can reliably identify and locate damaged components.

TELECOMMUNICATIONS

IMPORTANCE OF ASSURED TELECOMMUNICATIONS

Telecommunications plays a key role in US society in terms of its direct effect on individuals and business and due to its impact on other key infrastructures. The relationship of telecommunications to the other critical infrastructures, such as the financial industry, is often recognized during and following widespread outages, such as those experienced as a result of the September 11, 2001, attacks on the World Trade Centers and the immediate vicinity of "Ground Zero." The local disruption of all critical infrastructures, including power, transportation, and telecommunications, interrupted operations in key financial markets and posed increased liquidity risks to the US financial system.[1] In the days following the attacks, institutions in the affected areas were implementing their business continuity plans, which proved vital to the rapid restoration and recovery of services in the New York City area. In addition, the President emphasized that the prompt restoration of Wall Street's capabilities was critical to the economic welfare of the Nation; in doing so, he aptly linked economic stability to national security.

For some of the most critical infrastructure services, such as electric power, natural gas, and financial services, assured communications are essential to their recovery following a major adverse event. The importance of telecommunications in an emergency situation is underscored by the existence of the National Communications System (NCS), established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions,*[2] which include administering the National

---

[1] James J. MacAndrews and Simmon M. Potter, "Liquidity Effects of the Events of September 11, 2001," Federal Reserve Bank of New York Economic Policy Review, November 2002.

[2] The mission of the NCS shall be to assist the President, the National Security Council, the Homeland Security Council, the Director of the Office of Science and Technology Policy, and the Director of the Office of Management and Budget in: (1) the exercise of the telecommunications functions and responsibilities set forth in Section 2 of this Order; and (2) the coordination of the planning for and provision of national security and emergency preparedness communications for the Federal government under all circumstances, including crisis or emergency, attack, recovery, and reconstitution.

The NCS shall seek to ensure that a national telecommunications infrastructure is developed which: (1) Is responsive to the national security and emergency preparedness needs of the President and the Federal departments, agencies and other entities, including telecommunications in support of national security leadership and continuity of government; (2) Is capable of satisfying priority telecommunications requirements under all circumstances through use of commercial, government and privately owned telecommunications resources; (3) Incorporates the necessary combination of hardness, redundancy, mobility, connectivity, interoperability, restorability and security to obtain, to the maximum extent

Coordinating Center (NCC) for Telecommunications to facilitate the initiation, coordination, restoration, and reconstitution of National Security and Emergency Preparedness (NS/EP) telecommunications services or facilities under all crises and emergencies; developing and ensuring the implementation of plans and programs that support the viability of telecommunications infrastructure hardness, redundancy, mobility, connectivity, and security; and serving as the focal point for joint industry-government and interagency NS/EP telecommunications planning and partnerships. In addition, the President's National Security Telecommunications Advisory Committee (NSTAC), a Federal Advisory Committee Act (FACA) CEO-level advisory group to the President, is tasked with providing industry-sourced advice and expertise related to implementing policies affecting NS/EP communications. These NS/EP services are those "critical to the maintenance of a state of readiness or the response to and management of any event or crisis that causes harm or could cause harm to the population, damage to or the loss of property, or degrades or threatens the NS/EP posture of the United States."[3]

The NSTAC in its 1985 Report on EMP found that "consistent with its cost constraints, industry should incorporate low-cost EMP mitigation practices into new facilities and, as appropriate, into upgrade programs. For those areas where a carrier/supplier recognizes that a significant improvement in EMP resistance and surveillance could be achieved, but at a cost beyond the carrier/supplier's own cost constraints, the carrier/supplier should identify such options to the government for evaluation and possible funding." On October 9, 1985, the NSTAC approved the EMP Final Task Force Report and forwarded a recommendation to the President, calling for a joint industry and Government program to reduce the costs of existing techniques for mitigating high-altitude electromagnetic pulse (HEMP)-induced transients and to develop new techniques for limiting transient effects. As a result, the NCS and industry, working with the ATIS—the Alliance for Industry Solutions—developed a set of ANSI standards and Generic Requirements[4] to address EMP.[5]

---

practicable, the survivability of national security and emergency preparedness telecommunications in all circumstances, including conditions of crisis or emergency; and (4) Is consistent, to the maximum extent practicable, with other national telecommunications policies.

[3] NS/EP Implications for Electronic Commerce, NSTAC Report, June 1999.

[4] Telcordia GR-1089-CORE.

[5] ANSI T1.320.

NS/EP Definitions

NS/EP Telecommunications Services: Telecommunications services that are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) that causes or could cause injury or harm to the population, damage to or loss of property, or degrades or loss of property, or degrades or threatens the NS/EP posture of the United States. (*"Telecommunications Service Priority [TSP] System for National Security Emergency Preparedness: Service User Manual," NCS Manual 3-1-1, July 9, 1990. Appendix A.)*

NS/EP Requirements: Features that maintain a state of readiness or respond to and manage an event or crisis (local, national, or international), which causes or could cause injury or harm to the population, damage to or loss of property, or degrade or threaten the NS/EP posture of the United States. (*Federal Standard 1037C)*

With respect to NS/EP telecommunications, capabilities exist for prioritizing phone calls through the wireline, wireless, and satellite networks during the time interval when call volumes are excessive and facilities are damaged, giving priority to restoring services that may be damaged or degraded, and getting new circuits into operation.

According to recent testimony by a DHS official, "The NCS is continuing a diverse set of mature and evolving programs designed to ensure priority use of telecommunications services by NS/EP users during times of national crisis. The more mature services—including the Government Emergency Telecommunications Service (GETS) and the Telecommunications Service Priority (TSP)—were instrumental in the response to the September 11 attacks. FY 2005 funding enhances these programs and supports the development of the Wireless Priority Service (WPS) program and upgrade to the Special Routing Arrangement Service (SRAS). Specifically, priority service programs include: (1) GETS, which offers nationwide priority voice and low-speed data service during an emergency or crisis situation; (2) WPS, which provides a nationwide priority cellular service to key NS/EP users, including individuals from federal, state and local governments and the private sector; (3) TSP, which provides the administrative and operational framework for priority provisioning and restoration of critical NS/EP telecommunications services; (4) SRAS, which is a variant of GETS to support the Continuity of Government (COG) program including the reengineering of SRAS in the AT&T network and development of SRAS capabilities in the MCI and Sprint networks, and; (5) the Alerting and Coordination Network (ACN), which is an NCS program that

provides dedicated communications between selected critical government and telecommunications industry operations centers."[6]

For example, due to concerns with respect to getting calls through during intervals of high network call volumes that follow disaster events, the Nuclear Regulatory Commission (NRC) utilizes the Government Emergency Telecommunications System (GETS) and other NS/EP telecom services such as wireless priority services to communicate with commercial nuclear power plants and to relay critical status information. This use of GETS grew out of lessons learned from the Three Mile Island incident in 1979. During the initial days of this incident, NRC personnel experienced communication problems that were attributed primarily to call volume overload at the local telephone company switch.

Another NS/EP service is the Telecommunications Service Priority (TSP) program, which exists to assign priority provisioning and restoration of critical NS/EP telecommunications services in the hours immediately following a major disaster. In place since the mid-1980s, more than 50,000 circuits are protected today under TSP, including circuits associated with critical infrastructures such as electric power, telecommunications, and financial services.

The telecommunication system consists of four basic and primary physical systems: wireline, wireless, satellite, and radio. In general, the national telecommunications infrastructure may be farther advanced then others in its ability to address the particular consequences of EMP. This is due in large measure to the recognized alternative threats to this system, as well as broad recognition of its importance to society. The three primary and separate systems (excluding radio) that make up the broad telecommunications infrastructure each provide specialized services; they also overlap heavily. Thus the loss or degradation of any one of these somewhat redundant subsystems subjects the remaining functional subsystems to heavier service loads.

Each of these four primary systems is unique in their capability to suffer insult from EMP. The wireline system is robust but will be degraded within the area exposed to the EMP electromagnetic fields. The wireless system is technologically fragile in relation

[6] Statement of General Frank Libutti, Under Secretary for Information Analysis and Infrastructure Protection ,Department of Homeland Security, Before the House Homeland Select Subcommittee on Intelligence and Counterterrorism and the Subcommittee on Infrastructure and Border Security, March 4, 2004, p. 12.

to EMP, certainly in comparison to the wireline one. In general, it may be so seriously degraded in the EMP region as to be unavailable. Low Earth Orbit (LEO) communications satellites may also suffer radiation damage as a result of one or more high-altitude nuclear bursts that produce EMP (see Space Systems, page 44).

The radio communication sub-system of the national telecommunications infrastructure is not widespread, but where it is connected to antennas, power lines, telephone lines, or other extended conductors, it is also subject to substantial EMP damage. However, radio communication devices not so connected or not connected to such conductors at the time of the EMP attack are likely to be operable in the post-attack interval.

EMP Effects on Telecommunications

Based upon results of Commission-sponsored testing, an EMP attack would disrupt or damage a functionally significant fraction of the electronic circuits in the Nation's civilian telecommunications systems in the region exposed to EMP. The remaining operational networks would be subjected to high levels of call attempts for some period of time after the attack, leading to degraded telecommunications services.

Key government and civilian personnel will need priority access to use public network resources to coordinate and support local, regional, and national recovery efforts, especially during the interval of severe network congestion.

To offset the temporary loss of electric power, telecommunications sites now utilize a mix of batteries, mobile generators, and fixed-location generators. These typically have between 4 and 72 hours of backup power available, and thus will depend on either the resumption of electrical utility power or fuel deliveries to function for longer periods of time.

For some of the most critical infrastructure services such as electric power, natural gas, and financial services, assured communications are necessary—but aren't necessarily sufficient—to the survival of that service during the initial time-intervals after an EMP attack. Therefore, a systematic approach to protecting or restoring key communications systems will be required.

Recommended Mitigation Activities

The following actions are recommended as particularly effective ones for mitigating the impacts of EMP attack:

- Expand the respective roles of the National Communications System (NCS) and the Defense Threat Reduction Agency (DTRA) as the Federal Focal Point for EMP within the Code of Federal Regulations Part 215[7] to address infrastructure interdependencies related to NS/EP telecommunications services.
- Ensure services targeted at NS/EP operate effectively as new technology is introduced into the telecommunications network. Specifically, services such as Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS) that are intended for use in emergency situations to improve the call completion probabilities for key personnel must operate effectively. Within the next 15 years, new technologies will be introduced into the public networks that will play major roles in operation of these services. EMP is just one of the potential threats that could stress the telecommunications networks; therefore, ensuring that NS/EP services perform effectively as new technology is introduced has benefits beyond providing robustness to EMP, and moreover is consistent with avoiding failures from other hostile actions.
- Determine the effects of EMP on different types of telecommunication equipment and facilities, using tests and theoretical analyses of the type done in the course of Commission-sponsored work and previous EMP-related studies conducted by the National Communications System (NCS).[8.] A comprehensive, continuing telecommunications testing program,[9] along with the use of existing national and international standards,[10] may be a model activity that would be a key part of this overall National effort.
- Improve the ability of key network assets to survive HEMP. There are key elements in the network such as the Signal Transfer Points (STPs) in the signaling system (Signaling System 7 (SS7)), Home Location Register (HLR), and Visiting Location Register (VLR) in the wireless networks whose degradation can result in the loss of service to a larger number of users. Effective mitigation strategies include a combination of site hardening and installation of protective measures for the fast rise-time (E1) component of EMP.
- Improve the ability of telecommunications to withstand the sustained loss of utility-supplied electric power. This mitigation strategy would entail the use of best practices, review and improvement of existing programs such

[7] 47CFR, Section 215, designated The Executive Agent, NCS, is the focal point within the Federal Government for all EMP technical data and studies concerning NS/EP telecommunications.

[8] For example: The Effects of High-Altitude Electromagnetic Pulse (HEMP) on Telecommunications Assets, NCS Technical Information Bulletin 92-5, February 1992.

[9] Similar to that conducted in response to the Signaling System 7 outages of the early 1990's (which affected large portions of the United States) under the Inter-network Interoperability Test Program (IITP) of the Alliance for Telecommunications Industry Solutions (ATIS).

[10] Standards for Protection of Telecommunications Links, NCS Technical Notes, Volume 6, Number 3, 1999.

as the Telecommunications Electric Service Priority (TESP) program, and the increased use of alternative backup power sources.

- Conduct exercises to refine contingency operations. Conduct exercises that test and provide for improved contingency operations, assuming widespread multi-infrastructure degradation. The adequacy of mutual aid agreements, cross-organizational planning and coordination, and critical asset prioritization are examples of elements that should be tested and developed.
- Managers of these critical services must design their systems and operating procedures to take into account the potential vulnerabilities introduced by EMP-driven failure of telecommunications devices and sub-systems.

BANKING AND FINANCE

NATURE OF THE PROBLEM

The financial services industry comprises a network of organizations and attendant systems that process instruments of monetary value in the form of deposits, loans, funds transfers, savings, and other financial transactions. It includes banks and other depository institutions, including the Federal Reserve System; investment-related companies such as underwriters, brokerages, and mutual funds; industry utilities such as the New York Stock Exchange, the Automated Clearing House, and the Society for Worldwide Interbank Financial Telecommunications; and third party processors that provide electronic processing services to financial institutions, including data and network management and check processing.

Virtually all American economic activity depends upon the functioning of the financial services industry. Today, most financial transactions that express National wealth are performed and recorded electronically. Virtually all transactions involving banks and other financial institutions happen electronically. Essentially all record-keeping of financial transactions involves information stored electronically. The financial services industry has evolved to the point that it would be impossible to operate without the efficiencies, speeds, and processing and storage capabilities of electronic information technology.

The terrorist attacks of September 11, 2001, demonstrated the vulnerabilities arising from the significant interdependencies of the Nation's critical infrastructures. The attacks disrupted all critical infrastructures in New York City, including power, transportation, and telecommunications. Consequently, operations in key financial markets were interrupted, increasing liquidity risks for the United States financial system.[11]

The Interagency Paper,[12] which was jointly issued by the Office of the Comptroller of the Currency (OCC), the Federal Reserve Board (FRB), and the Securities and Exchange Commission (SEC), specifies clearing and settlement systems as the most

[11] James J. MacAndrews and Simmon M. Potter, "Liquidity Effects of the Events of September 11, 2001," Federal Reserve Bank of New York Economic Policy Review, November 2002.

[12] The Federal Reserve Board, the Office of the Comptroller of the Currency, and the Securities and Exchange Commission, *Interagency Paper on Sound Practices to Strengthen the Resilience of the US Financial System*, September 5, 2002.

critical business operations at risk for financial markets.[13] Because financial markets are highly interdependent, a wide-scale disruption of core clearing and settlement processes would have an immediate systemic effect on critical financial markets.[14]

> *Over the past couple of decades, the American economy has become increasingly resilient to shocks. Deregulated financial markets, far more flexible labor markets, and, more recently, the major advances in information technology have enhanced our ability to absorb disruptions and recover. In the past, our economy has quickly regained its previous levels following the devastation of hurricanes, earthquakes, floods, and myriad other natural disasters that periodically batter various regions of our country. Although the trauma of September 11 shares some characteristics with such disruptions, the differences are important. In contrast to natural disasters, last week's events are of far greater concern because they strike at the roots of our free society, one aspect of which is our market-driven economy. All modern economies require the confidence that free-market institutions are firmly in place and that commitments made today by market participants will be honored not only tomorrow, but for years into the future. The greater the degree of confidence in the state of future markets, the greater the level of long-term investment. The shock of September 11, by markedly raising the degree of uncertainty about the future, has the potential to result, for a time, in a pronounced disengagement from future commitments. And that, in the short run, would imply a lessened current level of activity. Indeed, much economic activity ground to a halt last week. But the foundations of our free society remain sound, and I am confident that we will recover and prosper as we have in the past. As a consequence of the spontaneous and almost universal support that we received from around the world, an agreement on a new round of multilateral trade negotiations now seems more feasible. Such an outcome would lead to a stronger global market system. A successful round would not only significantly enhance world economic growth but also answer terrorism with a firm reaffirmation of our commitment to open and free societies.*
>
> —Testimony of Chairman Alan Greenspan, *The condition of the financial markets* Before the Committee on Banking, Housing, and Urban Affairs, US Senate September 20, 2001

Moreover, in December 2002, the FRB revised its policy and procedures for NS/EP telecommunications programs administered by the National Communications System (NCS) to identify those functions supporting the Federal Reserve's NS/EP mission to maintain national liquidity.[15] The FRB expanded the scope of services that would seriously affect continued financial operations if a telecommunications disruption

[13] Ibid., pg. 5.

[14] Systemic risk includes the risk that the failure of one participant in a transfer system or financial market to meet its required obligations will cause other participants to be unable to meet their obligations when due, causing significant liquidity or credit problems or threatening the stability of financial markets. The use of the term "systemic risk" in this report is based on the international definition of systemic risk in payments and settlement systems provided in Committee on Payment and Settlement Systems, Bank for International Settlements, "A Glossary of Terms in Payment and Settlement Systems," 2001.

[15] *Federal Register*, vol. 67, no. 236, Monday, December 9, 2002. Notice, "Federal Reserve Board Sponsorship for Priority Telecommunication Services of Organizations That Are Important to National Security/ Emergency Preparedness," http://www.federalreserve.gov/boarddocs/press/other/2002/20021203/attachment.pdf.

of "a few minutes to one day" occurred.[16] These functions, which are listed below, require same-day recovery and are critical to the operation and liquidity of banks and the stability of financial markets:

- Large-value inter-bank funds transfer, securities transfer, or payment-related services, such as Fedwire, Clearing House Interbank Payments System (CHIPS), and the Society for Worldwide Interbank Financial Telecommunications (SWIFT)
- Automated clearinghouse (ACH) operators
- Key clearing and settlement utilities
- Treasury automated auction and processing system
- Large-dollar participants of these systems and utilities

The increasing dependence of the United States on an electronic economy, so beneficial to the creation and preservation of wealth, also adds to the adverse effects that would be produced by an EMP attack. The electronic technologies that are the foundation of the financial infrastructure are potentially vulnerable to EMP. These systems are also potentially vulnerable to EMP indirectly through other critical infrastructures, such as the electric power grid and telecommunications.

Recommended Mitigation and Responsibility

Securing the financial services industry from the EMP threat is vital to the national security of the United States. The Federal government must assure that this system can survive sufficiently to preclude serious, long-term consequences.

The Department of Homeland Security, the Federal Reserve Board, and the Department of the Treasury, in cooperation with other relevant agencies, must develop contingency plans to ride out and recover key financial systems promptly from an EMP attack.

Key financial services include those means and resources that provide the general population with cash, credit, and other liquidity required to buy food, fuel, and other essential goods and services. We must protect the Nation's financial networks, banking records, and data retrieval systems that support cash, check, credit, debit, and other transactions through judicious balance of hardening, redundancy, and contingency plans.

[16] Federal Reserve Board Sponsorship for Priority Telecommunications Services of Organizations That Are Important to National Security/Emergency Preparedness, *Federal Register*, Vol. 67, No. 236, Monday, December 2003, Notices, p. 72958.

The Federal government must work with the private sector to assure the protection and effective recovery of essential financial records and services infrastructure components from all deliberate adverse events, including EMP attack. Implementation of the recommendations made by the Department of the Treasury, the FRB, and the SEC in their *Interagency Paper on Sound Practices to Strengthen the Resilience of the US Financial System* to meet sabotage and cyber-threats that could engender requirements for protection and recovery should be expanded to include expeditious recovery from EMP attack:

- "Every organization in the financial services industry should identify all clearing and settlement activities in each critical financial market in which it is a core clearing and settlement organization or plays a significant role" that could be threatened by EMP attack.
- Industry should "determine appropriate recovery and resumption objectives for clearing and settlement activities in support of critical markets" following an EMP attack.
- Industry should be prepared to cope with an EMP attack by maintaining "sufficient geographically dispersed resources to meet recovery and resumption objectives…. Backup sites should not rely on the same infrastructure components (e.g., transportation, telecommunications, water supply, electric power) used by the primary site. Moreover, the operation of such sites should not be impaired by a wide-scale evacuation at or inaccessibility of staff that service the primary site."
- Industry should, "Routinely use or test recovery and resumption arrangements…. It is critical for firms to test backup facilities of markets, core clearing and settlement organizations, and third-party service providers to ensure connectivity, capacity, and the integrity of data transmission" against an EMP attack.

FUEL/ENERGY INFRASTRUCTURE

The vulnerabilities of this sector are produced by the responses of the electronic control systems that provide and utilize the near-real-time data flows needed to operate the fuel/energy infrastructure efficiently, as well as to identify and quickly react to equipment malfunctions or untoward incidents. EMP could also cause control or data-sensor malfunctions that are not easily discernible, leading to counterproductive operational decisions. Process control systems are critical to the operation and control of petroleum refineries, and little or no notice of an outage significantly increases the potential for damage during an emergency shutdown. Communications systems that are critical for operational control represent another locus of vulnerability. Communications are also critical in refineries to ensure safety of on-site personnel, the adjacent population, and the surrounding environment. The energy distribution infrastructure is also critically dependent on the availability of commercial power to operate the numerous pumps, valves and other electrical equipment that are required for a functional infrastructure.

DHS must develop a contingency plan that will provide strategy for protection and recovery for this sector, to include actions to be taken by both Government and industry. Government should establish a national inventory of parts for those items with long lead-times or that would be in demand in the event of a catastrophic event such as an EMP attack. The Energy Information Sharing and Analysis Center (ISAAC) should, with government funding, expand its mission to address EMP issues, and the government should work with the private sector to implement the general approach described in Strategy and Recommendations, page 11.

TRANSPORTATION INFRASTRUCTURE

NATURE OF THE PROBLEM

America's transportation sector is often addressed as a single infrastructure, but in reality its multiple modes provide for several separate infrastructures. Rail includes the freight railroad and commuter rail infrastructures; road includes the trucking and automobile infrastructures; water includes the maritime shipping and inland waterway infrastructures; and air includes the commercial and general aviation infrastructures.

As recognized by the President's National Security Telecommunications Advisory Committee (NSTAC) Information Infrastructure Group Report:[17]

- The transportation industry is increasingly reliant on information technology and public information-transporting networks.
- Although a nationwide disruption of the transportation infrastructure may be unlikely, even a local or regional disruption could have a significant impact. Due to the diversity and redundancy of the US transportation system, the infrastructure is not at risk of nationwide disruption resulting from information system failure. Nonetheless, a disruption of the transportation information infrastructure on a regional or local scale has potential for widespread economic and national security effects.
- Marketplace pressures and increasing utilization of IT make large-scale, multimodal disruptions more likely in the future. As the infrastructure becomes more interconnected and interdependent, the transportation industry will increasingly rely on information technology to perform its most basic business functions. As this occurs, it becomes more likely that information system failures could result in large-scale disruptions of multiple modes of the transportation infrastructure.

Electronics vulnerable to EMP permeate the transportation infrastructures.

- There is a need for a broad-based infrastructure assurance awareness program to assist all modes of transportation.
- The transportation industry could leverage ongoing research and development initiatives to improve the security of the transportation information infrastructure.

[17] *NSTAC Information Infrastructure Group Report*, June 1999, <http://www.ncs.gov/NSTAC/NSTACXXII/Reports/NSTAC22-IIG.pdf.

- There is a need for closer coordination between the transportation industry and other critical infrastructures.

The imperative to achieve superior performance has also led to a tremendous increase in the use of electronics that are potentially vulnerable to EMP. The internal combustion engine provides a familiar example of this phenomenon. Modern engines utilize electronics to increase performance, increase fuel efficiency, reduce emissions, increase diagnostic capability, and increase safety.

To gauge the degree of vulnerability of transportation infrastructures to EMP, the Commission has conducted an assessment of selected components of these infrastructures that are necessary to their operations. The assessment relied on testing where feasible, surveys and analyses for equipment and facilities for which testing was impractical, and reference to similarities to equipment for which EMP vulnerability data exists.

Based on this assessment, significant degradation of the transportation infrastructures are likely to occur in the immediate aftermath of an EMP attack. For example, municipal road traffic will likely be severely congested, possibly to the point of wide-area gridlock, as a result of traffic light malfunctions and the fraction of operating cars and trucks that will experience both temporary and in some cases unrecoverable engine shutdown. Railroad traffic will stop if communications with railroad control centers are lost or railway signals malfunction. Commercial air traffic will likely cease operations for safety and other traffic control reasons. Ports will stop loading and unloading ships until commercial power and cargo hauling infrastructures are restored.

The ability of the major transportation infrastructure components to recover depends on the plans in place and the availability of resources—including spare parts and support from other critical infrastructures upon which transportation is dependent. Transportation infrastructures have emergency response procedures in place; however, they do not explicitly address conditions that may exist for an EMP attack, such as little or no warning time and simultaneous disruptions over wide areas. Restoration times will depend on the planning and training carried out, and on the availability of services from other infrastructures—notably power, fuel, and telecommunications.

STRATEGY FOR PROTECTION AND RECOVERY

RAILROADS

Railroad operations are designed to continue under stressed conditions. Backup power and provisioning is provided for operations to continue for days or even weeks at reduced capacity. However, some existing emergency procedures, such as transferring

operations to backup sites, rely on significant warning time, such as may be received in a weather forecast before a hurricane. An EMP attack may occur without warning, thereby compromising the viability of available emergency procedures. Therefore, under the overall leadership of the DHS, the government and private sectors should work together to implement the general approach described in Strategy and Recommendations, page 11.

Specific actions should include:

- Heighten railroad officials' awareness of the possibility of EMP attack without warning that would produce wide-area, long-term disruption and damage to electronic systems.
- Perform test-based EMP assessments of railroad traffic control centers and retrofit modest EMP protection into these facilities, thereby minimizing the potential for adverse long term EMP effects. The emphasis of this effort should be on electronic control and telecommunication systems.

TRUCKING AND AUTOMOBILES

Emphasizing prevention and emergency clearing of traffic congestion in this area, DHS should coordinate a government and private sector program to:

- Initiate an outreach program to educate State and local authorities and traffic engineers on EMP effects and the expectation of traffic signal malfunctions, vehicle disruption and damage, and consequent traffic congestion.
- Work with municipalities to formulate recovery plans, including emergency clearing of traffic congestion and provisioning spare controller cards that could be used to repair controller boxes.
- Sponsor development of economical protection modules—preliminary results for which are already available from Commission-sponsored research—that could be retrofitted into existing traffic signal controller boxes and installed in new controller boxes during manufacture.
- Sponsor development of automobile robustness specifications and testing for EMP. These specifications should be implemented by augmenting existing specifications for gaining immunity to transient electromagnetic interference (EMI), rather than by developing separate specifications for EMP.

MARITIME SHIPPING

The essential port operations to be safeguarded are ship traffic control, cargo loading and unloading, and cargo storage and movement (incoming and outgoing). Ship traffic control is provided by the Coast Guard, which has robust backup procedures in

place. Cargo storage and movement are covered by other transportation infrastructure recommendations. Therefore, focusing on cargo operations in this area, DHS should coordinate a government and private sector program to:

- Heighten port officials' awareness of the wide geographic coverage of EMP fields, the risk due to loss of commercial power for protracted time-intervals, and the need to evaluate the practicality of providing emergency generators for at least some portion of port and cargo operations.
- Assess the vulnerability of electric-powered loading/unloading equipment. Review the electromagnetic protection already in place for lightning, and require augmentation of this protection to provide significant EMP robustness.
- Coordinate findings with the "real-time" repair crews to ensure they are aware of the potential for EMP damage. Based on the assessment results, recommend spares provisions so that repairs can be made in a timely manner.
- Assess port data centers for the potential loss of data in electronic media. Provide useful measures of protection against EMP causing loss of function and/or data.
- Provide protected off-line spare parts and computers sufficient for minimum essential operations.
- Provide survivable radio and satellite communication capabilities for the Coast Guard and the Nation's ports.

COMMERCIAL AVIATION

In priority order, it must be ensured that airplanes caught in the air during an EMP attack can land safely, that critical recovery assets are protected, and that contingency plans for an extended no-fly period are developed. Thus, DHS should coordinate a government program in cooperation with the FAA to perform an operational assessment of the air traffic control system to identify a "thin-line" that provides the minimal essential capabilities necessary to return the air traffic control capability to at least a basic level of service after an EMP attack. Based on the results of this operational assessment, develop tactics for protection, operational workarounds, spares provisioning, and repairs to return to a minimum-essential service level.

FOOD INFRASTRUCTURE

NATURE OF THE PROBLEM

EMP can damage or disrupt the infrastructure that supplies food to the population of the United States. Recent federal efforts to better protect the food infrastructure from terrorist attack tend to focus on preventing small-scale disruption of the food infrastructure, such as would result from terrorists poisoning some food. Yet an EMP attack could potentially disrupt the food infrastructure over a large region encompassing many cities for a protracted period of weeks to months.

Technology has made possible a dramatic revolution in US agricultural productivity. The transformation of the United States from a nation of farmers to a nation where less than 2 percent of the population is able to feed the other 98 percent and supply export markets is made possible only by technological advancements that, since 1900, have increased the productivity of the modern farmer by more than 50-fold. Technology, in the form of knowledge, machines, modern fertilizers and pesticides, high-yield crops and feeds, is the key to this revolution in food production. Much of the technology for food production directly or indirectly depends upon electricity, transportation, and other infrastructures.

The distribution system is a chokepoint in the US food infrastructure. Supermarkets typically carry only enough food to provision the local population for 1 to 3 days. Supermarkets replenish their stocks on virtually a daily basis from regional warehouses that usually carry enough food to supply a multi-county area for about one month. The large quantities of food kept in regional warehouses will do little to alleviate a crisis if it cannot be distributed to the population in a timely manner. Distribution depends largely on a functioning transportation system.

MITIGATION AND RESPONSIBILITY

Federal, state, and regional governments should establish plans for assuring that food is available to the general population in case of major disruption of the food infrastructure. Planning to locate, preserve, deliver, distribute, and ration existing stockpiles of processed and unprocessed food, including food stockpiled by the Department of Agriculture, Department of Defense, and other government agencies, will

be an important component of maintaining the food supply. Planning to protect, deliver, and ration food from regional warehouses, under conditions where an EMP attack has disrupted the power, transportation, and other infrastructures for a protracted period, should be a priority. Plans to process and deliver private and government grain stockpiles would significantly supplement the processed food stored in regional warehouses. According to the USDA's National Agricultural Statistical Service, total private grain stockpiles in the United States amount to over 255 million metric tons. Federal grain stockpiles held by the Commodity Credit Corporation exceed 1.7 million metric tons, with 1.6 million metric tons of that amount dedicated to the Bill Emerson Humanitarian Trust for Overseas Emergency. Planning should include an assessment of how much food the population of the United States would need in an emergency when the food infrastructure is disrupted for a protracted period. Food stockpiles should be increased if existing stockpiles of food appear to be inadequate.

Presidential initiatives have designated the Department of Homeland Security as the lead agency responsible for the security of the food infrastructure, overseeing and working with the Department of Agriculture. Currently, under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (the Stafford Act), the President "is authorized and directed to assure that adequate stocks of food will be ready and conveniently available for emergency mass feeding or distribution" in the United States. The Stafford Act should be amended to provide for plans to locate, protect, and distribute existing private and government stockpiles of food, and to provide plans for distribution of existing food stockpiles to the general population in the event of a national emergency.

WATER SUPPLY INFRASTRUCTURE

National-level responsibilities have already been assigned to the Department of Homeland Security (DHS) and the Environmental Protection Agency (EPA) to protect the water infrastructure from terrorist threats. A recent Presidential Directive establishes new national policy for protection of our Nation's critical infrastructures against terrorist threats that could cause catastrophic health effects.[18] EPA is the designated lead agency for protection of drinking water and water treatment systems. DHS and EPA should ensure that protection includes EMP attack among the recognized threats to the water infrastructure.

[18] Homeland Security Presidential Directive – 7, *Critical Infrastructure Identification, Prioritization, and Protection.* December 17, 2003.

EMERGENCY SERVICES

VULNERABILITIES

An EMP attack will result in diminished capabilities of emergency services during a time of greatly increased demand upon them. The EMP vulnerability of emergency services systems is primarily due to the susceptibility of computer and communications equipment, and secondarily due to likely commercial electric power outages. Recent test results indicate that some failures of computers and network equipment can be expected at low EMP field levels; at higher levels, much more pervasive equipment failures are expected. Mobile radio communications equipment can be expected to experience disruption and failure at EMP threat levels that are likely to be experienced. Moreover, emergency services are critically dependent on the commercial telephone network, on electric power, and thus on fuel for backup generators. Degradation in these capabilities following an EMP attack is likely, as discussed previously, thereby providing another source of cascading infrastructure failure.

RECOMMENDED STRATEGY FOR PROTECTION AND RECOVERY

The Department of Homeland Security must develop a strategy for protection and recovery of emergency services that emphasizes the inclusion of the EMP threat in planning and training and the establishment of technical standards for EMP protection of critical equipment. The Department of Homeland Security, including its Federal Emergency Management Agency (FEMA), and state and local governments should augment existing plans and procedures to address both immediate and long-term emergency services response to EMP attack. Plans should include provision for early warning notification, and a protection/recovery protocol based on graceful degradation and rapid recovery that emphasizes a balance between limited hardening and provisioning of spare components, as well as training for their use in emergency reconstitution. In addition, the Department of Homeland Security should provide technical support, guidance, and assistance to state and local governments, as well as to other federaldDepartments and agencies, to ensure the EMP survivability or rapid recovery of critical emergency services networks and equipment.

SPACE SYSTEMS

Over the past few years, there has been increased focus on US space systems in low Earth orbits and their unique vulnerabilities, among which is their susceptibility to nuclear detonations at high altitudes—the same events that produce EMP. It is also important to include, for the protection of a satellite-based system in any orbit, its control system and ground infrastructure, including up-link and down-link facilities.

Commercial satellites support many significant services for the Federal government, including communications, remote sensing, weather forecasting, and imaging. The national security and homeland security communities use commercial satellites for critical activities, including direct and backup communications, emergency response services, and continuity of operations during emergencies. Satellite services are important for national security and emergency preparedness telecommunications because of their ubiquity and separation from other communications infrastructures.

The Commission to Assess United States National Security Space Management and Organization conducted an assessment of space activities that support US national security interests, and concluded that space systems are vulnerable to a range of attacks due to their political, economic, and military value.[19] Satellites in low Earth orbit generally are at very considerable risk of severe lifetime degradation or outright failure from collateral radiation effects arising from an EMP attack on ground targets.

The Department of Homeland Security and the Department of Defense should jointly execute a systematic assessment of the significance of each space system, particularly those in low Earth orbits, to missions such as the continuity of government, strategic military force protection, and the protection of critical tactical force support functions. Information from this assessment and associated cost and risk judgments will inform senior government decision making regarding protection and performance-assurance of these systems, so that missions can be executed with the required degrees of surety in the face of the possible threats.

[19] *Report of the Commission to Assess United States National Security Space Management and Organization,* January 11, 2001.

GOVERNMENT

DHS should give priority to measures to ensure that the President and other senior Federal officials can exercise informed leadership of the Nation in the aftermath of an EMP attack, and to improving post-attack response capabilities at all levels of government.

The President, Secretary of Homeland Security, and other senior officials must be able to manage the national recovery in an informed and reliable manner. Current national capabilities were developed for Cold War scenarios in which it was imperative that the President have assured connectivity to strategic retaliatory forces. While this is still an important requirement, there is a new need for considerably broader, robust connectivity between national leaders, government at all levels, and key organizations within each infrastructure sector so that the status of infrastructures can be assessed in a reliable and comprehensive manner and their recovery and reconstitution intelligently managed. The Department of Homeland Security, working through the Homeland Security Council, should give high priority to identifying and achieving the minimum levels of robust connectivity needed for recovery following EMP attack. In doing this, DHS should give particular emphasis to exercises that evaluate the robustness of the solutions being implemented.

Working with state authorities and private-sector organizations, the Department of Homeland Security should develop draft protocols for implementation by emergency and other government responders following EMP attack, Red Team these extensively, and then institutionalize validated protocols through issuance of standards, training, and exercises.

KEEPING THE CITIZENRY INFORMED

Support to National leadership also involves measures to ensure that the President can communicate effectively with the citizenry. Although the US can improve prevention, protection, and recovery in the face of an EMP attack to levels below those that would have catastrophic consequences for the Nation, an EMP attack would still cause substantial disruption, even under the best of circumstances. Many citizens would be without power, communications and other services for days—or perhaps substantially longer—before full recovery could occur. During that interval, it will be crucial to provide a reliable channel of information to those citizens to let them know what has happened, the current situation, when help of what types for them might be available, what their governments are doing, and the host of questions which, if not answered, are certain to create more instability and suffering for the affected individuals, communities, and the Nation as a whole.

PROTECTION OF MILITARY FORCES

The end of the Cold War relaxed the discipline for achieving EMP survivability within the Department of Defense, and gave rise to the perception that an erosion of EMP survivability of military forces was an acceptable risk. EMP simulation and test facilities have been mothballed or dismantled, and research concerning EMP phenomena, hardening design, testing, and maintenance has been substantially decreased. However, the emerging threat environment, characterized by a wide spectrum of actors that include near-peers, established nuclear powers, rogue nations, sub-national groups, and terrorist organizations that either now have access to nuclear weapons and ballistic missiles or may have such access over the next 15 years have combined to place the risk of EMP attack and adverse consequences on the US to a level that is not acceptable.

Current policy is to continue to provide EMP protection to strategic forces and their controls; however, the end of the Cold War has relaxed the discipline for achieving and maintaining that capability within these forces. The Department of Defense must continue to pursue the strategy for strategic systems to ensure that weapons delivery systems of the New Triad are EMP survivable, and that there is, at a minimum, a survivable "thin-line" of command and control capability to detect threats and direct the delivery systems. The Department of Defense has the capability to do this, and the costs can be within reasonable and practical limits.

The situation for general-purpose forces (GPF) is more complex. The success of these forces depends on the application of a superior force at times and places of our choosing. We accomplish this by using a relatively small force with enormous technological advantages due to superior information flow, advanced warfighting capabilities, and well-orchestrated joint combat operations. Our increasing dependence on advanced electronics systems results in the potential for an increased EMP vulnerability of our technologically advanced forces, and if unaddressed makes EMP employment by an adversary an attractive asymmetric option.

The United States must not permit an EMP attack to defeat its capability to prevail. The Commission believes it is not practical to protect all of the tactical forces of the US and its coalition partners from EMP in a regional conflict. A strategy of replacement and reinforcement will be necessary. However, there is a set of critical capabilities that is essential to tactical regional conflicts that must be available to these

reinforcements. This set includes satellite navigation systems, satellite and airborne intelligence and targeting systems, an adequate communications infrastructure, and missile defense.

The current capability to field a tactical force for regional conflict is inadequate in light of this requirement. Even though it has been US policy to create EMP-hardened tactical systems, the strategy for achieving this has been to use the DoD acquisition process. This has provided many equipment components that meet criteria for durability in an EMP environment, but this does not result in confidence that fielded forces, as a system, can reliably withstand EMP attack. Adherence to the equipment acquisition policy also has been spotty, and the huge challenge of organizing and fielding an EMP-durable tactical force has been a disincentive to applying the rigor and discipline needed to do so.

EMP durability should be provided to a selected set of tactical systems such that it will be practical to field tactical forces that cannot be neutralized by an EMP attack. The Department of Defense must perform a capabilities-based assessment of the most significant EMP threats to its tactical capabilities and develop strategies for coping with these threats in a reliable and effective manner.

Overall, little can be accomplished without the sustained attention and support of the leadership of the Department of Defense and Congress. This will require the personal involvement and cooperation among the Secretary of Defense, the Chairman of the Joint Chiefs, the Service Chiefs, and the appropriate congressional oversight committees in creating the necessary climate of concern; overseeing the development of strategy; and reaffirming the criticality of survivable and endurable military forces, including command, control, and communications (C3) in updated policy guidance, implementation directives, and instructions. Congressionally mandated annual reports from the Secretary of Defense and the Chairman of the Joint Chiefs on the status and progress for achieving EMP survivability of our fighting forces will emphasize the importance of the issue and help ensure that the necessary attention and support of the DoD leadership continues.

APPENDIX A
THE COMMISSION AND ITS METHOD

The Commission used a capability-based methodology to estimate potential EMP threats over the next 15 years.[1] The objective was to identify the range of plausible adversary EMP attack capabilities that cannot be excluded by prudent decision makers responsible for national and homeland security.

Bases for this assessment included current intelligence estimates of present and near-term military capabilities; current and past engineering accomplishments (what are adversaries likely to be capable of achieving, given accomplishments in other programs at comparable stages of development?); and trends impacting adversary military capabilities through 2018. In line with its capabilities-based approach, the Commission did not attempt to establish the relative likelihood of EMP strikes versus other forms of attack.

> ***...a tendency in our planning to confuse the unfamiliar with the improbable. The contingency we have not considered looks strange; what looks strange is therefore improbable; what seems improbable need not be considered seriously.***
>
> —Thomas C. Schelling, Foreword, in Roberta Wohlstetter, Pearl Harbor: Warning and Decision, Stanford University Press, 1962, p. vii.

Intelligence community organizations and the National Nuclear Security Administration's nuclear weapon laboratories (Lawrence Livermore, Los Alamos, and Sandia) provided excellent technical support to the Commission's analyses.[2] The Institute for Defense Analyses hosted and developed technical analyses for the Commission. While it benefited from these inputs, the Commission developed an independent assessment. Views expressed in this report are solely attributable to the Commission.

The Russian Federation (RF) has a sophisticated understanding of EMP that derives in part from the test era when the Soviet Union did high-altitude atmospheric tests

[1] Rob Mahoney, Capabilities-Based Methodology for Assessing Potential Adversary Capabilities, March 2004.

[2] The Commission's report and associated documents provide the necessarily classified assessments of future adversary capabilities for EMP attack and weapon issues.

over its own territory, impacting civilian infrastructures. To benefit from Russian expertise, the Commission:

- Sponsored research projects at Russian scientific institutions.
- Hosted a September 2003 US/RF symposium on EMP at which presentations were given by Russian general officers.
- Sponsored a December 2003 technical seminar on EMP attended by scientists from the Russian Federation and the United States.

The Commission also reviewed additional relevant foreign research and programs and assessed foreign perspectives on EMP attacks.

In considering EMP, the Commission also gave attention to the coincident nuclear effects that would result from a detonation that produces EMP, e.g., possible disruption of the operations of, or damage to, satellites in space.

Different types of nuclear weapons produce different EMP effects. The Commission limited its attention to the most strategically significant cases in which detonation of one or few nuclear warheads could result in widespread, potentially long-duration disruption or damage that places at risk the functioning of American society or the effectiveness of US military forces.

In addition to examining potential threats, the Commission was charged to assess US vulnerabilities (civilian and military) to EMP and to recommend measures to counter EMP threats. For these purposes, the Commission reviewed research and best practices within the United States and other countries. Early in this review it became apparent that only limited EMP vulnerability testing had been accomplished for modern electronic systems and components. To partially remedy this deficit, the Commission sponsored illustrative testing; results are presented in the Commission's report.

Commissioners brought to this task a wide range of expertise, including service as an advisor to the President; senior management experience in both civilian and military agencies, national laboratories, and the corporate sector; and technical expertise in the design of nuclear weapons and in the hardening of systems against nuclear weapon effects.

APPENDIX B
COMMISSIONERS

Dr. William R. Graham is Chairman of the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack. He is also Chairman of the Board and Chief Executive Officer of National Security Research Inc. (NSR), a Washington-based company that conducts technical, operational, and policy research and analysis related to US national security. In the recent past he has served as a member of several high-level study groups, including the Department of Defense Transformation Study Group, the Commission to Assess United States National Security Space Management and Organization (the Rumsfeld Commission on Space), and the Commission to Assess the Ballistic Missile Threat to the United States (also led by Hon. Donald Rumsfeld). From 1986–89 Dr. Graham was the director of the White House Office of Science and Technology Policy while he served concurrently as Science Advisor to President Reagan, Chairman of the Federal Joint Telecommunications Resources Board, and member of the Arms Control Experts Group. For 11 years he served as a member of the Board of Directors of the Watkins-Johnson Company.

Dr. John S. Foster, Jr., is Chairman of the Board of GKN Aerospace Transparency Systems, chairman of Technology Strategies and Alliances, and consultant to Northrop Grumman Corporation, Sikorsky Aircraft Corp., Ninesigma, and Defense Group. He retired from TRW as Vice President, Science and Technology, in 1988 and continued to serve on the Board of Directors of TRW from 1988 to 1994. Dr. Foster was Director of Defense Research and Engineering for the Department of Defense from 1965–1973, serving under both Democratic and Republican administrations. In other distinguished service, Dr. Foster has been on the Air Force Scientific Advisory Board, the Army Scientific Advisory Panel, and the Ballistic Missile Defense Advisory Committee, Advanced Research Projects Agency. Until 1965, he was a panel consultant to the President's Science Advisory Committee, and from 1973–1990 he was a member of the President's Foreign Intelligence Advisory Board. He is a member of the Defense Science Board, which he chaired from January 1990–June 1993. From 1952–1962, Dr. Foster was with Lawrence Livermore National Laboratory (LLL), where he began as a Division Leader in experimental physics, became Associate Director in 1958, and became Director of LLL and Associate Director of the Lawrence Berkeley National Laboratory in 1961.

Mr. Earl Gjelde is the Managing Director and Chief Executive Officer of Summit Group International, Ltd.; Summit Energy Group, Ltd.; Summit Energy International 2000, LLC; and Summit Power NW, LLC, primary participants in the development of over 5,000 megawatts of natural gas fired electric and wind generating plants within the United States. He has also held a number of government posts, serving as President George Herbert Walker Bush's Under (now called Deputy) Secretary and Chief Operating Officer of the US Department of the Interior (1989) and as President Ronald Reagan's Under Secretary and Chief Operating Officer of the US Department of the Interior (1985–1988). While in the Reagan administration he served concurrently as Special Envoy to China (1987), Deputy Chief of Mission for the US-Japan Science and Technology Treaty (1987–1988), and Counselor for Policy to the Director of the National Critical Materials Council (1986–1988); the Counselor to the Secretary and Chief Operating Officer of the US Department of Energy (1982-1985); and Deputy Administrator,

Chief Operating Officer, and Power Manager of the Bonneville Power Administration (1980-1982). Prior to 1980, he was a principal officer of the Bonneville Power Administration.

Dr. Robert J. Hermann is a senior partner of Global Technology Partners, LLC, a Boston-based investment firm that focuses on technology, defense aerospace, and related businesses worldwide. In 1998, Dr. Hermann retired from United Technologies Corporation, where he was Senior Vice President, Science and Technology. Prior to joining UTC in 1982, Dr. Hermann served 20 years with the National Security Agency with assignments in research and development, operations, and NATO. In 1977, he was appointed Principal Deputy Assistant Secretary of Defense for Communications, Command, Control, and Intelligence. In 1979, he was named Assistant Secretary of the Air Force for Research, Development, and Logistics and concurrently was Director of the National Reconnaissance Office.

Mr. Henry (Hank) M. Kluepfel is a Corporate Vice President for Corporate Development and Chief Scientist in the Enterprise Security Solutions Group of SAIC. He is the company's leading cyberspace security advisor to the President's National Security Telecommunications Advisory Committeel (NSTAC) and the Network Reliability and Interoperability Council (NRIC). Mr. Kluepfel is widely recognized for his 30-plus years of experience in security technology research, design, tools, forensics, risk reduction, education, and awareness, and he is the author of industry's de facto standard security base guideline for the Signaling System Number 7(SS7) networks connecting and controlling the world's public telecommunications networks. In past affiliations with Telcordia Technologies (formerly Bellcore), AT&T, BellSouth and Bell Labs, he led industry efforts to protect, detect, contain, and mitigate electronic and physical intrusions and led the industry's understanding of the need to balance technical, legal, and policy-based countermeasures to the then emerging hacker threat. He is recognized as a Certified Protection Professional by the American Society of Industrial Security and is a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE).

General (USAF, Ret.) Richard L. Lawson is Chairman of Energy, Environment and Security Group, Ltd., and former President and CEO of the National Mining Association. He also serves as Vice Chairman of the Atlantic Council of the U.S; Chairman of the Energy Policy Committee of the US Energy Association; Chairman of the United States delegation to the World Mining Congress; and Chairman of the International Committee for Coal Research. Active duty positions included serving as Military Assistant to the President; Chief of Staff, Supreme Headquarters Allied Powers Europe; Director for Plans and Policy, Joint Chiefs of Staff; Deputy Director of Operations, Headquarters US Air Force; and Deputy Commander in Chief, US European Command.

Dr. Gordon K. Soper is Group Vice President of Defense Group Inc., responsible for broad direction of corporate goals relating to company support of government customers in areas of countering the proliferation of weapons of mass destruction, chemical/biological defense and domestic preparedness, treaty verification research, nuclear arms control and development of new business areas and growth of technical staff. He provides senior-level technical support on a range of task areas to the Defense Threat Reduction Agency (DTRA), the Chemical and Biological National Security Program of National Nuclear Security Administration, and the Counterproliferation and Chem/Bio Defense Office of the Office of the Secretary of Defense. Previously, Dr. Soper was Principal Deputy to the Assistant to the Secretary of Defense for Nuclear, Chemical and Biological Defense Programs (ATSD (NCB); Director, Office of Strategic and Theater Nuclear Forces Command, Control and Communications (C3) of the Office of the

Assistant Secretary of Defense (C3I); and Associate Director for Engineering and Technology/Chief Scientist at the Defense Communications Agency.

Dr. Lowell L. Wood, Jr., is a member of the Technical Advisory Group, US Senate Select Committee on Intelligence; a member of the Undersea Warfare Experts Group, US House of Representatives Committee on Armed Services; a visiting fellow at the Hoover Institution and 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 Director's technical staff, University of California Lawrence Livermore National Laboratory, where he has held numerous positions since 1972.

Dr. Joan Woodard is Executive Vice President and Deputy Director of Sandia National Laboratories, responsible for all of Sandia's programs, operations, staff, and facilities. She is also responsible for the laboratory's strategic planning. Prior to her current appointment, Dr. Woodard was Vice President of the Energy, Information and Infrastructure Technology Division, where her responsibilities included energy-related projects in fossil energy, solar, wind, geothermal, geosciences, fusion, nuclear power safety and severe accident analysis, and medical isotope processing; environment-related programs in remediation, nuclear waste management and repository certification, and waste minimization; information technology programs in information surety, command and control systems, and distributed information systems; and programs responsible for security of the transportation of nuclear weapons and special nuclear materials, and safety of commercial aviation. Over 80% of the programs included industrial or academic partners, and the nature of the work ranged from basic research to prototype systems evaluation.