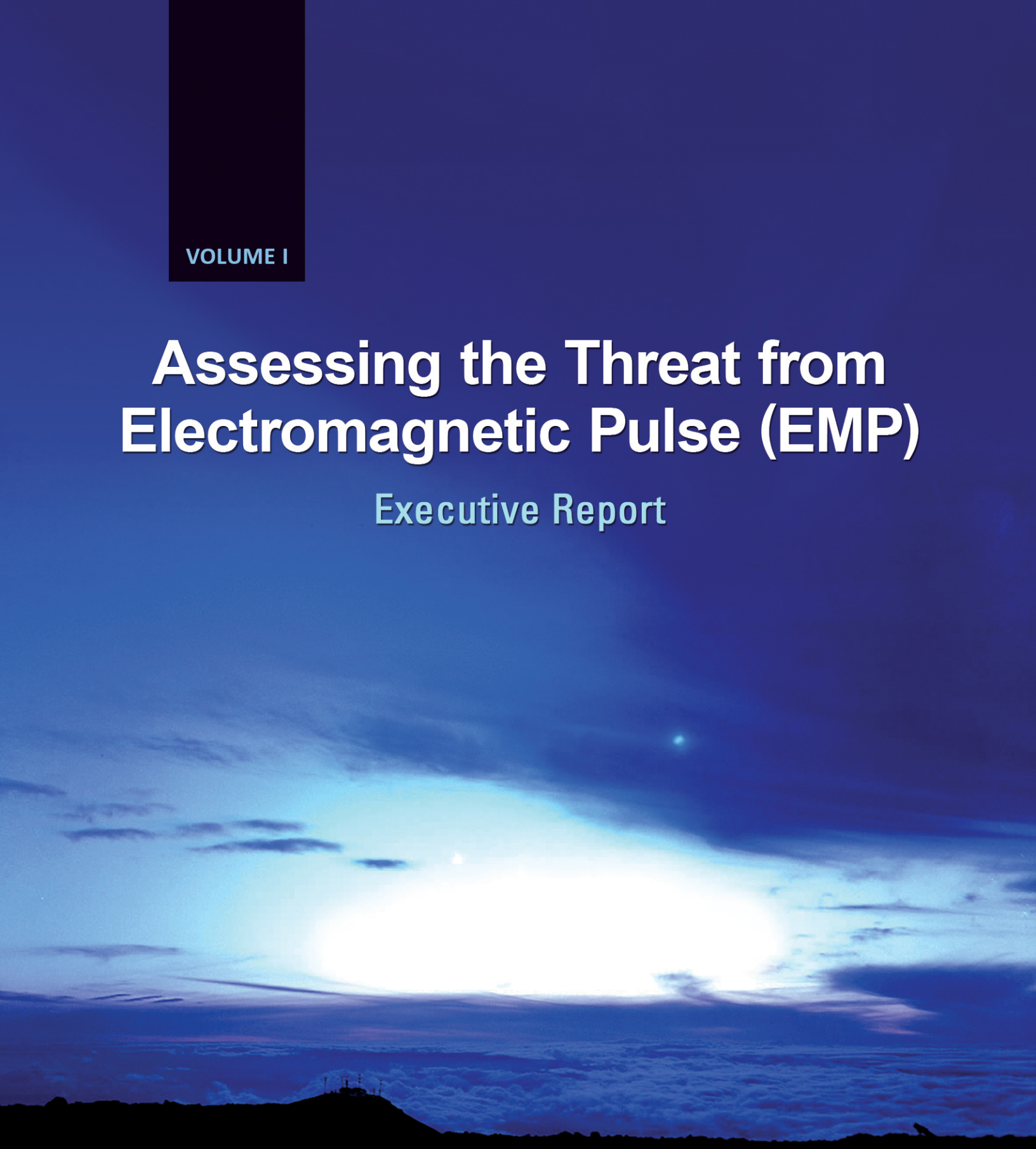
VOLUME I

Assessing the Threat from Electromagnetic Pulse (EMP)

Executive Report



JULY 2017

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

Assessing the Threat from Electromagnetic Pulse (EMP)

Executive Report

July 2017

REPORT OF THE COMMISSION TO ASSESS THE THREAT TO THE UNITED STATES FROM ELECTROMAGNETIC PULSE (EMP) ATTACK

The cover photo depicts Fishbowl Starfish Prime at 0 to 15 seconds from Maui Station in July 1962, courtesy of Los Alamos National Laboratory.

This report is a product of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. The Commission was established by Congress in the FY2001 National Defense Authorization Act, Title XIV, and was continued per the FY2016 National Defense Authorization Act, Section 1089.

The Commission completed its information-gathering in June 2017. The report was cleared for open publication by the DoD Office of Prepublication and Security Review on April 9, 2018.

This report is unclassified and cleared for public release.

TABLE OF CONTENTS

EXECUTIVE SUMMARY 1
OBSERVATIONS, ANALYSIS, AND RECOMMENDATIONS 4
The EMP Threat 4
Barriers to Effective Protection from EMP 6
Late-Time EMP Fields and Effects (E3) 13
Testing Selected EMP-vulnerable Full-system Equipment to Failure 15
Intelligence Community Assessment of the EMP Threat 16
CONCLUSIONS 17

APPENDIX A Legislation Re-establishing the Commission 19
APPENDIX B High Altitude Nuclear Explosion-Generated Electromagnetic Effects 20

BIOGRAPHIES 22
Commissioners 22
Senior Advisors 24

COMMISSION REPORTS 27

ACRONYMS AND ABBREVIATIONS

DHS	Department of Homeland Security
DoD	Department of Defense
DOE	Department of Energy
DOT	Department of Transportation
ELECTRA	Electromagnetic Effects Comparison Test and Reliability Assessment
EMP	electromagnetic pulse
EPA	Environmental Protection Agency
FAA	Federal Aviation Administration
FDA	Food and Drug Administration
FERC	Federal Energy Regulatory Commission
HEMP	high-altitude electromagnetic pulse
NERC	North American Electric Reliability Corporation
NRC	Nuclear Regulatory Commission

PREFACE

The Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack (herein and elsewhere referred to as "the EMP Commission") was re-established by the National Defense Authorization Act (NDAA) for Fiscal Year 2016 on November 25, 2015, and funded by the appropriation for the Commission on December 18, 2015. Delays by the Department of Defense in providing funding, clearance support, and contractor support to the Commission throughout 2016 delayed the first meeting until January 2017. The Commission's statutory mandate terminated at the end of June 2017 in accord with the terms of the NDAA. EMP is a complex subject, and the DoD provided only limited support beyond this time to allow the Commission to complete its work even though funding to continue was available. As a result, the Commission could not adequately complete the full scope of the Congressional charge as described in Appendix A. This report is therefore necessarily limited, yet the Commission is confident this material contained herein is accurate and trusts it is valuable to the recipients.

Following the last meeting of the EMP Commission on June 8-9, 2017, global events have strengthened public awareness of the worldwide vulnerability of critical infrastructures to high altitude EMP. North Korean state news, KCNA, displayed photos of an alleged thermonuclear weapon and claimed on September 3, 2017, "The H-bomb, the explosive power of which is adjustable from tens of kilotons to hundreds of kilotons, is a multi-functional thermonuclear nuke [sic] with great destructive power which can be detonated even at high altitudes for super-powerful EMP (electromagnetic pulse) attack according to strategic goals." The United States, its territories, and allies are therefore the target of current threats by the government of North Korea that specifically include EMP, and also include further development and exploitation of high altitude EMP weapons.

EXECUTIVE SUMMARY

The critical national infrastructure in the United States faces a present and continuing existential threat from combined-arms warfare, including cyber and manmade electromagnetic pulse (EMP) attack, as well as from natural EMP from a solar superstorm. During the Cold War, the U.S. was primarily concerned about an EMP attack generated by a high-altitude nuclear weapon as a tactic by which the Soviet Union could suppress the U.S. national command authority and the ability to respond to a nuclear attack—and thus negate the deterrence value of assured nuclear retaliation. Within the last decade, newly-armed adversaries, including North Korea, have been developing the ability and threatening to carry out an EMP attack against the United States. Such an attack would give countries that have only a small number of nuclear weapons the ability to cause widespread, long-lasting damage to critical national infrastructures, to the United States itself as a viable country, and to the survival of a majority of its population.

Major efforts have been undertaken by the Department of Defense to assure that the U.S. national command authority and U.S. strategic forces could survive and operate after an EMP attack. However, no major efforts were thought necessary to protect critical national infrastructures, relying on nuclear deterrence to protect them. With the development of small nuclear arsenals and long-range missiles by small, hostile, and potentially irrational adversaries, including North Korea, the threat of a nuclear EMP attack against the U.S. becomes one of the few ways that such a country could inflict devastating damage to the United States. It is critical, therefore, that the U.S. national leadership address the EMP threat as a critical and existential issue, and give a high priority to assuring the leadership is engaged and the necessary steps are taken to protect the country from EMP. Otherwise, foreign adversaries may reasonably consider such an attack as one which can gravely damage the U.S. by striking at its technological Achilles' heel without having to engage the U.S. military.

Protecting and defending the national electric grid and other critical infrastructures from cyber and EMP could be accomplished at reasonable cost and minimal disruption to the present systems that comprise U.S. critical infrastructure. This is commensurate with Trump Administration plans to repair and improve U.S. infrastructures, increase their reliability, and strengthen homeland defense and military capability. Continued failure to address the U.S. vulnerability to EMP generated by a high-altitude nuclear weapon invites such an attack.

The single most important action *that requires immediate action* to advance U.S. security and survivability is that the President establish an Executive Agent with the authority, accountability, and resources to manage U.S. national infrastructure protection and defense against the existential EMP threat (*Recommendation 1*). Current institutional authorities and responsibilities—government, industry, regulatory agencies—are fragmented, incomplete,

under-resourced, and unable to protect and defend against foreign hostile EMP threats or solar superstorms.

The Commission highly commends President Trump's Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, signed on May 11, 2017. **The Commission strongly recommends that implementation of cybersecurity for the electric grid and other critical infrastructures include EMP protection** *(Recommendation 2)*, because all-out cyber warfare may well include nuclear EMP attack. Protecting against nuclear EMP will also protect against natural EMP from solar storms, although the converse is not true. The United States must take steps to mitigate its current state of vulnerability to these well-known natural and adversary EMP threats. To further this endeavor, **the Commission encourages the President to work with Congressional leaders to establish a joint Presidential-Congressional Commission, with its members charged with supporting the Nation's leadership to achieve, on an accelerated basis, the protection of critical national infrastructures**. *(Recommendation 3)*.

Across the U.S. government, the DoD and its supporting laboratories and contractors have by far the most knowledge, data, and experience related to the production of and survival from nuclear weapon-generated EMP. However, the DoD has largely failed to make this knowledge available to other government agencies and to the organizations that develop, build, and operate U.S. critical national infrastructure. For example, there has been a continuing unwillingness of the DoD to provide specific information about the EMP environment to the commercial community owing to classification restrictions. Today the DHS looks to the DOE to provide guidance and direction for protecting the national electric power grids. Such a course of action would take longer and cost more compared to establishing a program of cooperation with the knowledgeable parts of the DoD.

In the absence of an unclassified, well-informed U.S. late-time (E3) EMP threat specification [described in Appendix B], electric utilities, electrical equipment manufacturers, and electric research institutes have articulated their inability to design appropriate countermeasures and to justify cost recovery for capital investments programs. Accordingly, this Commission has prioritized the development of late-time E3 threat specifications, derived from openly available test data. As part of this assessment, Commission staff analyzed E3 EMP measurements from two nuclear high-altitude tests performed by the Soviet Union in 1962. Physicists with extensive experience in EMP modeling used these data waveforms and an understanding of the scaling relationships for the nuclear explosion-induced upper atmospheric heave phenomenon that produces the E3 EMP electromagnetic fields by disturbing the natural magnetic field of the Earth. Based on this analysis, **the Commission recommends that government agencies and industries adopt new standards to protect critical national infrastructures from damaging E3 EMP heave fields, with more realistic standards of 85 V/km** *(Recommendation 4).* Typical waveforms for commercial applications are included in Appendix B that should prove useful for the protection of the national power grids. **The Commission also recommends**

electric grid equipment with long-replacement times such as large power transformers be tested to system failure *(Recommendation 5).*

In the area of national intelligence, the Commission found that the classified report by the Joint Atomic Energy Intelligence Committee (JAEIC) on EMP issued in 2014 is factually erroneous and analytically unsound. **The Commission recommends the Director of National Intelligence circulate to all recipients of the 2014 JAEIC report the EMP Commission critique of that report and direct a new assessment be prepared that supersedes the 2014 JAEIC EMP report** *(Recommendation 6)*. The new report should be reviewed by experts in the subject areas being addressed and circulated to all the recipients of the 2014 assessment.

OBSERVATIONS, ANALYSIS, AND RECOMMENDATIONS

The Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack was previously convened by the Congress from 2001-2005 and from 2007-2008, and currently from 2016-2017.[1,2]

The current Commission assessment is consistent with the previous recommendations. In summary, the Commission sees the high-altitude nuclear explosion-generated electromagnetic pulse as an existential threat to the survival of the United States and its allies that can be exploited by major nuclear powers and small-scale nuclear weapon powers, including North Korea and non-state actors, such as nuclear-armed terrorists.

THE EMP THREAT

The United States—and modern civilization more generally—faces a present and continuing existential threat from naturally occurring and manmade electromagnetic pulse assault and related attacks on military and critical national infrastructures. A nationwide blackout of the electric power grid and grid-dependent critical infrastructures—communications, transportation, sanitation, food and water supply—could plausibly last a year or longer.[3] Many of the systems designed to provide renewable, stand-alone power in case of an emergency, such as generators, uninterruptable power supplies (UPS), and renewable energy grid components, are also vulnerable to EMP attack.[4]

A long-term outage owing to EMP could disable most critical supply chains, leaving the U.S. population living in conditions similar to centuries past, prior to the advent of electric power.[5] In the 1800s, the U.S. population was less than 60 million, and those people had many skills and assets necessary for survival without today's infrastructure. An extended blackout today could result in the death of a large fraction of the American people through the effects of societal collapse, disease, and starvation. While national planning and preparation for such events could help mitigate the damage, few such actions are currently underway or even being contemplated.

---

1 The EMP Commission has previously published two unclassified reports: *Executive Report* dated 2004, and *Critical National Infrastructures*, dated 2008.

2 See Appendix A, "Legislation Re-establishing the Commission," National Defense Authorization Act for Fiscal Year 2016, Sec. 1089.

3 For example, see E. Conrad, G. Gurtman, G. Kweder, M. Mandell, and W. White. *Collateral Damage to Satellites from an EMP Attack,* Report to the EMP Commission, DTRA-IR-10.22.

4 Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. *HEMP Direct Drive Testing of Sample Solar Systems.* Report of the EMP Commission. July 2017.

5 National Security Telecommunications Advisory Committee (NSTAC). *People and Processes: Current State of Telecommunications and Electric Power*, January 31, 2006.

Combined-arms cyber warfare, as described in the military doctrines of Russia, China, North Korea, and Iran, may use combinations of cyber-, sabotage-, and ultimately nuclear EMP-attack to impair the United States quickly and decisively by blacking-out large portions of its electric grid and other critical infrastructures.[6] Foreign adversaries may aptly consider nuclear EMP attack a weapon that can gravely damage the U.S. by striking at its technological Achilles Heel, without having to confront the U.S. military. The synergism of such combined arms is described in the military doctrines of all these potential adversaries as the greatest revolution in military affairs in history—one which projects rendering obsolete many, if not all, traditional instruments of military power.

Any of several threats, as described here, must be considered:

- Solar superstorms can generate natural EMP over remarkably wide areas. Recurrence of the Carrington Event of 1859 is considered by many to be inevitable.[7] NASA estimates the likelihood of such an event to be 10 to 12 percent per decade, making it very likely that Earth will be affected by a solar superstorm within a matter of decades.[8] Such an event could blackout electric grids and other life-sustaining critical infrastructures, putting at risk the lives of many millions.
- Nuclear EMP attack might be conducted with only a single nuclear weapon detonated at high altitude or a few weapons at several hundred kilometers. These could be delivered by satellite, by a wide variety of long- and short-range missiles, including cruise and anti-ship missiles, by a jet doing a zoom-climb, or even by a high-altitude balloon. Some modes of attack could be executed relatively anonymously, thereby impairing deterrence.
- Russia, China, and North Korea now have the capability to conduct a nuclear EMP attack against the U.S. All have practiced or described contingency plans to do so.[9] Terrorists or other less-sophisticated actors also might mount a nuclear EMP attack if

---

6 For example, see Army of the Islamic Republic of Iran, Passive Defense: Approach to the Threat Center (Tehran: Martyr Lt. General Sayad Shirazi Center for Education and Research, Spring 2010); Shen Weiguang, World War, the Third World War—Total Information Warfare; General Vladimir Slipchenko, Non-Contact Wars (Moscow: January 1, 2000) translated in FBIS CEP20001213000001; and comments on North Korean state news on 3 September 2017.

7 R.A. Lovett. "What if the biggest solar storm on record happened today?" National Geographic News, March 4, 2011.

8 P. Riley and J.J. Love, "Extreme geomagnetic storms: Probabilistic forecasts and their uncertainties," Space Weather, v. 15, Jan. 2017, pp. 53-64. The probability of an extreme geomagnetic storm on the scale of the Carrington event varies based on the type of distribution used in the analysis from 3 (lognormal) to 10 (power law) per decade; see also P. Riley, "On the probability of occurrence of extreme space weather," Space Weather, v. 10, Feb. 2012, pp. 2101-2114, which estimates 12 percent per decade.

9 For example, see Army of the Islamic Republic of Iran, Passive Defense: Approach to the Threat Center (Tehran: Martyr Lt. General Sayad Shirazi Center for Education and Research, Spring 2010); Shen Weiguang, World War, the Third World War—Total Information Warfare; General Vladimir Slipchenko, Non-Contact Wars (Moscow: January 1, 2000) translated in FBIS CEP20001213000001; and comments on North Korean state news on 3 September 2017.

they have access to a suitable nuclear explosive. For missile delivery, no re-entry system or accurate missile guidance would be necessary.

- Cyber-attack, using computer viruses and related means, might be able to blackout much of the national electric grid for extended intervals. According to U.S. Cyber Command, Russia and China currently have such capability and it may only be a matter of time before other adversaries also gain a similar capability.[10]
- The U.S. electrical grid could be sabotaged by damaging extra-high-voltage (EHV) transformers using rifles, explosives, or non-nuclear EMP or directed energy weapons. Attacking less than a dozen key substations could result in protracted and widespread blackouts, according to the public statements of a past Chairman of the U.S. Federal Energy Regulatory Commission (FERC).[11] At least one substantive rehearsal of such an attack may have already taken place, at the Metcalf substation in the San Francisco Bay area.[12]
- The Commission highly commends President Trump's Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" signed on May 11, 2017. Including the potential for EMP as part of a cyber-attack is prudent when the current vulnerability of the U.S. electrical grid and critical infrastructures is taken into account.

Recommendation 2: *The Commission strongly recommends that implementation of cybersecurity for the electric grid and other critical infrastructures include EMP protection.*

BARRIERS TO EFFECTIVE PROTECTION FROM EMP

The government's response to the EMP Commission recommendations made in 2008 is not encouraging.

In a 2011 study, the DoD's JASON advisory panel concluded that the federal response to the EMP risk "is poorly organized; no one is in charge, resulting in duplications and omissions between agencies."[13]

---

10 Admiral Michael Rogers, Director, National Security Agency and Commander, U.S. Cyber Command. "Cybersecurity Threats: The Way Forward," Testimony, House Permanent Select Committee on Intelligence, Nov. 20, 2014.

11 R. Smith. "U.S. Risks National Blackout From Small-Scale Attack," Wall Street Journal, March 12, 2014; and R. Smith. "How America Could Go Dark," Wall Street Journal, July 14, 2016.

12 R. Smith. "Assault On California Power Station Raises Alarm On Potential For Terrorism," Wall Street Journal, February 5, 2014.

13 MITRE, 2011. Impacts of Severe Space Weather on the Electric Grid, MITRE, 2011, Report JSR-11-320.

A survey of recent government reports that address the protection of critical infrastructure reveals that none mention EMP, although critical infrastructure risks, resilience, protection, and availability are central to each report and to each Departments' mission.[14]

During a hearing before the Senate Homeland Security and Government Affairs (SHSGA) Committee on July 22, 2015, the U.S. Government Accountability Office (GAO) acknowledged that none of the recommendations of the EMP Commission to protect the national grid from EMP have been implemented by DHS, DOE, U.S. FERC or the North American Electric Reliability Corporation (NERC).[15] The GAO report explained lack of progress in protecting the national electric grid from EMP as due to a lack of leadership, because no one was in charge of solving the EMP problem, as follows: "DHS and DOE, in conjunction with industry, have not established a coordinated approach to identifying and implementing key risk management activities to address EMP risks."[16]

In March 2016, GAO reported that none of the essential measures recommended by the EMP Commission to protect the national electric grid had been addressed by Federal agencies, as shown in Table 1. The report stated that agencies had primarily drafted industry standards and federal guidelines and have only completed related research reports rather than implementing the resulting recommendations.[17]

Table 1: Status of Previous Recommendations from the EMP Commission

Recommendation	*Action*
Expand and extend emergency power supplies	None
Extend black start capability	None
Prioritize and protect critical nodes	None
Expand and assure intelligent islanding capability	None
Assure protection of high-value generation assets	None
Assure protection of high-value transmission assets	None
Assure sufficient numbers of adequately trained recovery personnel	None

Some efforts have been made, but these have been frustrated by a lack of leadership. For example, in October 2016, President Obama issued a comprehensive Executive Order for

---

[14] These reports include ***Mitigation of Power Outage Risks for Department of Defense Facilities and Activities 2015***, ***National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience*** (DHS), and ***U.S. Department of Energy Strategic Plan 2014-2018.***

[15] The Nuclear Regulatory Commission could be added to the list of deficient government agencies in that it has failed to similarly protect the nuclear power reactors and spent fuel storage facilities for which they are responsible.

[16] U.S. Senate Committee on Homeland Security and Governmental Affairs. Full committee hearing on "Protecting the Electric Grid from the Potential Threats of Solar Storms and Electromagnetic Pulse," held July 22, 2015.

[17] Government Accountability Office. *Critical Infrastructure Protection: Federal Agencies Have Taken Actions To Address Electromagnetic Risks, But Opportunities Exist To Further Assess Risks And Strengthen Collaboratio*n, GAO-16-243, March 2016.

coordinating efforts to prepare the nation for space weather events.[18] The primary federal mechanism for coordination is the interagency Space Weather Operations, Research, and Mitigation (SWORM) task force. This Executive Order gave DHS overall leadership in geomagnetic disturbance preparedness and the DOE leadership in addressing grid impacts, yet neither department has yet done a credible job of preparing the U.S. for such storms. This minimal effort did not address preparing the nation for similar wide-area effects on the electric power grid caused by an EMP attack.

Despite advocacy for a combined standard to protect the U.S. bulk power system from both man-made EMP and natural occurring solar storms, FERC in May 2013 ordered development of operating procedures and hardware protection standards only for solar geomagnetic disturbances.[19] Upon recommendations of the designated Electric Reliability Organization, NERC, FERC issued guidance for operational procedures to cope with solar storms in FERC Order 779.[20] These procedures excluded owner-operator requirements to protect generating facilities with generator step-up transformers, even those that have experienced transformer fires and explosions in prior solar storms. After development of a benchmark model by a NERC Geomagnetic Disturbance Task Force, in September 2016 FERC issued a standard for phased assessments of potential hardware protections that utilities would perform over a period of years, but without any mandatory hardware-protection installations actually required. [21]

These scattered, incoherent, and inadequate responses are a clear indication that for at least the last decade, critical national infrastructure protection from EMP has been largely ignored or dismissed by major departments of the U.S. government. The unaddressed vulnerability of the U.S. to EMP is an incentive for hostile powers to attack or, at a minimum, to develop capabilities for HEMP attack.

Interagency Cooperation and Centralized Governance

The DoD has, since 1962, understood the data, phenomena, magnitude, and importance of high-altitude electromagnetic pulse (HEMP) effects, and has applied that knowledge to certain military systems.[22] However, DoD has not adequately transferred that knowledge to other agencies of the government and to organizations that provide critical national infrastructures, such as electrical power and communications utilities. This is surprising because

---

18 The White House. “Coordinating Efforts to Prepare the Nation for Space Weather Events,” Executive Order 13744, October 13, 2016.

19 FERC Order No. 779, Reliability Standards for Geomagnetic Disturbances, May 16, 2013.

20 FERC Order No. 797, Reliability Standard for Geomagnetic Disturbance Operations, June 19, 2014.

21 FERC Order No. 830, Reliability Standard for Transmission System Planned Performance for Geomagnetic Disturbance Events, September 22, 2016. On the last full day of the Obama Administration, FERC denied four appeals for rehearing of Order 830, in FERC Order No. 830-A, January 19, 2017.

22 Operation Fishbowl in 1962 was the last high-altitude nuclear test series conducted by the U.S. military.

the DoD depends upon these same critical national infrastructures for domestic military operations as well as the security of the nation. To the contrary, the DoD has withheld public distribution of and has classified much of the data and technology that underlies protection against EMP even though potential adversaries of the U.S. are generally familiar with such technology. It is interesting to note that some of the most useful data available for predicting the electromagnetic fields produced by a nuclear explosion have been derived from data published by the former Soviet Union.[23]

In the absence of technology transfer and other support by the DoD to other agencies of the government and the industries supporting critical national infrastructures, the DHS depends upon the DOE, as their Sector-Specific Agency, to provide guidance and direction for protecting the national electric power grids.[24] The DOE relies on the National Laboratories under its sponsorship to provide such guidance and direction. While it is possible to conduct new testing and analysis required to generate the data, such a course of action would take longer and cost more compared to establishing a program of cooperation with the knowledgeable offices and laboratories in the DoD. A more efficient alternative is establishing a DoD policy that makes much of the defense-controlled data concerning EMP technology available to the government agencies and industry that support the U.S. critical national electric power infrastructure.

Regulatory Conflicts of Interest

The current institutional arrangements for protecting and improving the reliability of the electric grids and other critical infrastructures through the FERC and the NERC are not designed to address major national security threats to the electric power grids and other national critical infrastructures. Using FERC and NERC to achieve this level of national security has proven to be ineffectual. New institutional arrangements are needed to advance preparedness to guard against EMP and related threats to our critical national infrastructures.

The current U.S. power industry is largely self-regulated under FERC, NERC, Nuclear Regulatory Commission (NRC), and the electric power industry companies. The EMP Commission assesses that the existing regulatory framework for safeguarding the security and reliability of the electric power grid, which is based upon a partnership between the U.S. Government's FERC and the private non-profit NERC representing the utilities, is not set up to protect the U.S. against hostile EMP attack. For example, the standards for protecting the power grids from geomagnetic disturbances caused by solar storms prescribe threat levels

---

23 One of the best references for understanding and protecting against EMP is a translation of a Soviet handbook, entitled, "The Physics of Nuclear Explosions," Ministry of Defense of the Russian Federation, Central Institute of Physics and Technology, Volumes 1 and 2, ISBN 5-02-015124-6, 1997.

24 See the DHS Energy Sector overview at https://www.dhs.gov/energy-sector

below those recorded during major storms of historical record.[25] In May 2013, FERC ordered entities in the bulk power system to develop reliability standards to protect against solar geomagnetic disturbances (GMD). Generator operators were excluded. Despite multiple requests for FERC to develop a joint reliability standard for grid protection from both EMP and GMD hazards, NERC has only proposed limited standards for solar storm protection.[26,27] This can be attributed to the industry's desire to minimize protection requirements.

In public testimony before Congress, FERC has stated that it lacks regulatory power to compel NERC and the electric power industry to protect the grid from natural and nuclear EMP and other threats.[28] Consider the contrast in regulatory authority of the U.S. Federal Energy Regulatory Commission and similar regulatory agencies in the U.S. Government:

- The NRC has regulatory power to compel the nuclear power industry to incorporate nuclear reactor design features to make nuclear power safe. (To date, however, the NRC has not incorporated EMP survival criteria into design regulations. Further, that Commission has not required that spare transformers or emergency diesel generators be certified to be EMP-protected.)
- The U.S. Federal Aviation Administration (FAA) has regulatory power to compel the airline industry to ground aircraft considered unsafe, to change aircraft operating procedures considered unsafe, and to make repairs or improvements to aircraft in order to protect the lives of airline passengers.
- The U.S. Department of Transportation (DOT) has regulatory power to compel the automobile industry to install on cars safety glass, seatbelts, and airbags in order to protect the lives of the driving public.
- The U.S. Food and Drug Administration (FDA) has power to regulate the quality of food and drugs, and can ban under criminal penalty the sale of products deemed by the FDA to be unsafe to the public.
- The U.S. Environmental Protection Agency (EPA) has power to regulate clean air, clean water, and hazardous materials deemed by the EPA to be unsafe to the public.

---

25 J.G. Kappenman and W. Radasky, *Examination of NERC GMD Standards and Validation of Ground Models and Geo-Electric Fields,* Report to the EMP Commission, July 28, 2017. See also Foundation for Resilient Societies, Comments Submitted on Reliability Standard for Transmission System Planned Performance for Geomagnetic Disturbance Events, FERC Docket No. RM15-11-000, July 27, 2015; supplementary comments submitted August 10, 2015.

26 Requests for rehearing of Order No. 830 were filed by the Foundation for Resilient Societies, Edison Electric Institute, Center for Security Policy, and Jewish Institute for National Security Affairs. These were denied in Docket No. RM15-11-001, issued January 19, 2017.

27 U.S. Federal Energy Regulatory Commission. "Reliability Standard for Transmission System Planned Performance for Geomagnetic Disturbance Events," Docket No. RM15-11-000; Order No. 830, issued January 21, 2016.

28 Testimony of Joseph McClelland, U.S. FERC's Director of the Office of Electric Reliability, before the Senate Committee on Energy and Natural Resources (July 17, 2012); T. Sanders, "FERC's McClelland Calls For Enhanced Authority On Cyber-Security" Washington Energy Report, July 20, 2012.

Unlike the NRC, FAA, DOT, FDA, EPA, and most other U.S. government regulatory agencies, FERC does not have legal authority to compel the industry it is charged to regulate to act in the public interest. The U.S. FERC even lacks legal power to direct the electric utilities to install devices to protect the grid.

Currently, U.S. FERC only has the power to require NERC to propose a standard to protect the grid. NERC Standards are approved, or rejected, or remanded for further consideration by its membership, which is largely made up of representatives from the electric power industry. Once NERC proposes a standard to FERC, FERC cannot modify the standard, but must either accept or reject the proposed standard. If FERC rejects the proposed standard, NERC goes back to the drawing board, and the process starts all over again, often resulting in long delays for implementation of standards.

The DOE Quadrennial Energy Review released in January 2017 recommended, "… in the area of cybersecurity, Congress should provide FERC with authority to modify NERC-proposed reliability standards—or to promulgate new standards directly—if it finds that expeditious action is needed to protect national security in the face of fast-developing new threats to the grid. This narrow expansion of FERC's authority would complement DOE's national security authorities related to grid-security emergencies affecting critical electric infrastructure and defense-critical electricity infrastructure…"[29]

It is notable that this proposal would limit additional FERC authority to strengthen a reliability standard or to promulgate a new standard "in the area of cybersecurity." Although EMP hazards were not explicitly included in the proposed supplemental FERC authorities, EMP could be included under the cyber threat rubric as it directly debilitates cyber electronic systems.

Moreover, testifying before a House Energy and Commerce Subcommittee on February 1, 2017, the Chief Executive Officer of NERC expressed opposition to any Congressional grant of new FERC legislative authority to strengthen or directly promulgate any new grid reliability standard that NERC had not already proposed, thereby undermining the FERC's ability to protect the U.S. electric power grids from EMP attack.[30]

The geomagnetic disturbance standards proposed by the NERC, which the FERC has adopted to date, substantially underestimate the magnitude of historical and future geomagnetic disturbances. No standards for protecting the grid against nuclear or non-nuclear EMP weapons have been proposed or adopted.[31]

---

29 U.S. Department of Energy, *Transforming the Nation's Electricity System: The Second Installment of the QER*, January 2017, pp. S-16 and 7-7.

30 G.W. Cauley, *Hearing on the Electricity Sector's Efforts to Respond to Cybersecurity Threats*, Testimony before the House Subcommittee on Energy, Energy and Commerce Committee, February 1, 2017.

31 Federal Energy Regulatory Commission (FERC) Order 779, *Final Rule on Reliability Standard for Geomagnetic Disturbances*, Reliability Standard EOP-010-1, June 25, 2014; FERC Order 830, *Transmission System Planned*

Recommendations to Improve Governance

The Commission's chief recommendation is made to address the critical leadership deficiency.

> ***Recommendation 1:*** *The Commission recommends the President establish an Executive Agent with the authority, accountability, and resources to manage U.S. national infrastructure protection and defense against the existential EMP threat.*

The 2017 Presidential initiative to repair and strengthen U.S. infrastructure, cyber security, homeland defense, and military capability presents a unique opportunity to include measures for EMP protection that could obviate the existential threats from solar superstorms and combined-arms cyber warfare.

A second recommendation in the area of governance is to ensure a whole-of-government approach to the challenge of EMP protection. A joint Presidential-Congressional Commission on critical infrastructure protection could engage the free world's preeminent experts on EMP and related threats to serve the interagency in a manner akin to other advisory Commissions. For example, between 1947 and 1974, the Atomic Energy Commission advised the administration on how to attain most quickly and most cost-effectively the protection essential to long-term national survival and well-being. Such a structure would help the U.S. move beyond the current state of vulnerability to well-understood natural and man-made EMP threats.

> ***Recommendation 3:*** *The Commission encourages the President to work with Congressional leaders to establish a joint Presidential-Congressional Commission, with its members charged with supporting the Nation's leadership to achieve, on an accelerated basis, the protection of critical national infrastructures.*

Protecting the national electric grid and other critical infrastructures from the most severe of these threats—nuclear EMP attack—could be done in ways that protect against or significantly mitigate some other threats. Extensively tested, performance-proven technologies for EMP hardening have been developed and used by the DoD to protect critical military systems for over 50 years, and can be affordably adapted to protect electric grids and other critical infrastructures, at low-cost relative to that of an EMP catastrophe.

For example, the EMP Commission estimated in its 2008 report, critical parts of the national electric grid could be protected for about $2 billion.

Performance for Geomagnetic Disturbance Events, Reliability Standard TPL-007-1, Sep. 22, 2016, and FERC Order 830-A, *Denying Rehearing (of Order 830)*, January 19, 2017.

The U.S. knowledge base on EMP threat levels and waveforms is adequate. Likewise, EMP protection engineering is mature such that system protection programs can proceed immediately, without the need for lengthy additional research. The Commission is concerned that DOE and the Electric Power Research Institute (EPRI) are pursuing lengthy research and development programs to redefine environments and determine EMP system effects that introduce unnecessary delays in actual implementation of grid protection. The Commission finds that diverting these resources to pilot demonstration programs to protect selected sectors of the electric power grid would better serve the intent to protect the U.S. electrical grid. A strategic plan, along with the leadership to implement it, is needed now.

LATE-TIME EMP FIELDS AND EFFECTS (E3)

Solar superstorms, more formally called coronal mass ejection events, produce fields similar to EMP E3 effects. A NASA analysis states that "historical aurora records suggest a return period of 50 years for Québec-level storms and 150 years for very extreme storms, such as the 1859 Carrington event."[32] A high-altitude nuclear EMP event would also include higher frequency E1 and E2 fields. An understanding of the range of fields produced is required to understand their effects and the threat to the electrical grid.

To study the impact of these types of electromagnetic fields on extended electrical and communications transmission lines associated with the critical infrastructures, utilities need upper-bound, open-source information for the late-time (E3) high-altitude electromagnetic pulse threat waveform and its ground pattern. This need arises because of the effect of very low frequency electric field component (E3) coupled to horizontal electrical conductors, such as power transmission lines, that induce large quasi-direct current in those lines. When the quasi-direct current travels through the windings of large transformers handling high levels of power, they shift the magnetic field operating point in the core of the transformers, causing the transformer to generate abnormal harmonic waveforms that neither the transformer nor the electrical power system are able to manage. This results in overheating and damage to the transformers. Therefore, it is important that an unclassified bounding-case E3 waveform be available to those working in the commercial power equipment development and operation sectors.

While the DoD has developed high-altitude EMP waveforms (E1, E2, and E3) for its purposes, these are classified and not available for commercial use. The DoD policy of keeping its E3 threat specifications classified, and therefore not available to designers and operators of the U.S. national power grids, is, in the view of the Commission, much more damaging to the protection of U.S. critical national electrical power infrastructure than its release would be helpful to U.S. adversaries. Some potential adversaries, including Russia, have collected some of the

[32] T. Phillips. "Near Miss: The Solar Superstorm of July 2012." Science@NASA, July 23, 2014

best E3 data during their high altitude nuclear tests and therefore are already aware of the magnitude of the E3 fields. The withholding of E3 information is a DoD policy that is neither in the interest of U.S. national security and survival, nor in the interest of the DoD, because the DoD depends on commercial power for many of its activities.

In the absence of an unclassified, well-informed E3 specification, the Commission tasked experts to assess the openly available E3 HEMP measurements from two nuclear high-altitude tests performed by the Soviet Union in 1962. Using these data and an understanding of the scaling relationships for the E3 HEMP heave phenomenon, bounding waveforms for commercial applications were developed.

Because the measured quantities during these tests were the magnetic fields, it is possible for technologists familiar with electromagnetic theory to compute the E3 electric fields, using known ground conductivity profiles. Other ground conductivity profiles could lead to even higher fields, but some of these profiles do not cover a very large area of the Earth.

After computing the electric fields using the Soviet measurements, the results were scaled to account for the fact that the Soviet measurement locations were not at the optimum points on the ground to capture the maximum peak fields. This process determined that the scaled maximum peak E3 EMP heave field would have been 66 volts per kilometer (V/km) for the magnetic latitude of the Soviet tests.

The measured results were also evaluated for the E3 EMP heave field. This parameter increases for burst points closer to the geomagnetic equator, displaying inverse latitude behavior compared to solar GMD fields. This scaling increases the maximum peak electric field up to 85 V/km for locations in the southern continental United States, and 102 V/km for locations near the geomagnetic equator, such as Hawaii. The levels in Alaska would be lower, with a peak value of 38 V/km. While as noted these are not worst-case levels, they are reasonable upper-bound values useful in designing, evaluating, and operating bulk electrical power transmission systems and long-haul copper and fiber communication and data networks.[33]

> ***Recommendation 4:*** *The Commission recommends that government agencies and industries adopt new standards to protect critical national infrastructures from damaging E3 EMP heave fields, with more realistic standards of 85 V/km.*

Typical waveforms for commercial applications are included in Appendix B that should prove useful for the protection of the national power grids.

---

[33] Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. *Recommended E3 HEMP Heave Electric Field Waveform for the Critical Infrastructures*. Report of the EMP Commission, July 2017.

TESTING SELECTED EMP-VULNERABLE FULL-SYSTEM EQUIPMENT TO FAILURE

Some equipment that is essential for operation of critical infrastructures may be more economically stockpiled and stored in EMP-shielded structures than redesigned to be EMP-hardened. Other equipment with long replacement times or uncertainty of availability after an EMP attack will require EMP-hardening against E1, E2 and E3 hazards. While modeling of EMP vulnerability and mitigation measures is desirable, there is no substitute for full system testing to failure to project the likely post-EMP attack operability or prompt recovery of critical infrastructure equipment.

The Defense Nuclear Agency and its successor Defense Special Weapons Agency sponsored an innovative EMP evaluation program called the Electromagnetic Effects Comparison Test and Reliability Assessment (ELECTRA) from 1992 to 1995. ELECTRA performed both pre-test expert assessments of EMP survivability and system tests to failure using actual threat-level illumination and current injection testing. The ELECTRA Technical Review Group compared sealed-envelope analytical predictions of system EMP effects against post-test system effects.[34] Key findings from ELECTRA are pertinent to development of reliable and cost-effective EMP equipment protection and recovery programs.

The ELECTRA forecasting and test assessment program demonstrated that EMP system effects were most pronounced for modern electronic systems having unprotected external power and signal lines.[35] Moreover, forecasts by EMP survivability experts of pass-fail testing outcomes were no better than random coin-tossing when assessing actual system failures. Predictions of whether or not EMP effects would occur were frequently wrong and predictions for EMP current and voltage stress were subject to large errors (up to +/- 30 dB). System failures were predicted when none occurred, and conversely, no failures were predicted in cases where effects did occur. Pre-test predictions often missed the location—box, component—of system failure. The ELECTRA Technical Review Group concluded that methods used to predict EMP effects in a specific system that are based primarily on analysis or low-level testing are not reliable and recommended,

> *Where reliable [electromagnetic effects] predictions for specific systems are required, protections should be based on high-level functional-response tests performed on the specific systems of interest.*[36]

---

34 The ELECTRA Program's Technical Review Group's interim report of January 1995 includes a set of unclassified chapters on program methodology. See G.H. Baker, P. Castillo, C. McDonald, *et al.*, Electromagnetic Effects Comparison Test and Reliability Assessment (ELECTRA) Program: Executive Summary (U).

35 ELECTRA Executive Summary (1995), p. iv.

36 ELECTRA Executive Summary (1995), p. 49.

Further, where one or several complex system samples are subjected to high-level EMP injection testing, the test results can be prudently attributed to the larger population.[37] Thus, threat-level testing of even one sample is helpful to characterize the vulnerability and survivability of the larger set of systems. For large power transformers operating at 345 kV, 500 kV, and 765 kV voltages, for example, the DoD has the capability to transport EMP injection and diagnostic monitoring equipment to sites where these units are deployed. *In situ* testing to failure of exemplars of the major types of large power transformers under load would confirm whether specific types of large power transformers require EMP-protective equipment and enable new type transformer designs that resist EMP effects.

> ***Recommendation 5:*** *The Commission recommends that the Department of Defense and the Department of Energy provide expedited threat-level, full-system testing of large power transformers in wide use within the bulk electric system and share key findings with the electric utility industry.*

INTELLIGENCE COMMUNITY ASSESSMENT OF THE EMP THREAT

Finally, the Commission found that the classified report by the Joint Atomic Energy Intelligence Committee (JAEIC) on EMP issued in 2014 is factually erroneous and analytically unsound.[38] We recommend that the DNI circulate to all recipients of the 2014 JAEIC report the EMP Commission critique and direct a new assessment be prepared, reviewed by experts in the subject areas being addressed, and circulated to all the recipients of the 2014 assessment.

> ***Recommendation 6:*** *The Commission recommends the Director of National Intelligence circulate to all recipients of the 2014 JAEIC report the EMP Commission critique and direct a new assessment be prepared that supersedes the 2014 JAEIC EMP report.*

---

37 ELECTRA Executive Summary (1995), p. ii

38 Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. *Assessment of the 2014 JAEIC Report on High-altitude EMP Threats,* Report of the EMP Commission, July 2017.

CONCLUSIONS

The critical national infrastructure in the United States faces a present and continuing existential threat from combined-arms warfare, including cyber and manmade electromagnetic pulse (EMP) attack, as well as from natural EMP from a solar superstorm. During the Cold War, major efforts were undertaken by the Department of Defense to assure that the U.S. national command authority and U.S. strategic forces could survive and operate after an EMP attack. However, no major efforts were then thought necessary to protect critical national infrastructures, relying on nuclear deterrence to protect them. With the development of small nuclear arsenals and long-range missiles by new, radical U.S. adversaries, the threat of a nuclear EMP attack against the U.S. becomes one of the few ways that such a country could inflict devastating damage to the United States. It is critical, therefore, that the U.S. national leadership address the EMP threat as a critical and existential issue, and give a high priority to assuring the leadership is engaged and the necessary steps are taken to protect the country from EMP.

Protecting and defending the national electric grid and other critical infrastructures from cyber and EMP could be accomplished at reasonable cost and minimal disruption to the present systems that comprise U.S. critical infrastructure. The following six recommendations are offered to accomplish this goal.

Recommendation 1: *The Commission recommends the President establish an Executive Agent with the authority, accountability, and resources to manage U.S. national infrastructure protection and defense against the existential EMP threat.*

Recommendation 2: *The Commission strongly recommends that implementation of cybersecurity for the electric grid and other critical infrastructures include EMP protection.*

Recommendation 3: *The Commission encourages the President to work with Congressional leaders to establish a joint Presidential-Congressional Commission, with its members charged with supporting the Nation's leadership to achieve, on an accelerated basis, the protection of critical national infrastructures.*

Recommendation 4: *The Commission recommends that government agencies and industries adopt new standards to protect critical national infrastructures from damaging E3 EMP heave fields, with more realistic standards of 85 V/km.*

Recommendation 5: *The Commission recommends that the Department of Defense and the Department of Energy provide expedited threat-level, full-system testing of large power transformers in wide use within the bulk electric system and share key findings with the electric utility industry.*

Recommendation 6: *The Commission recommends the Director of National Intelligence circulate to all recipients of the 2014 JAEIC report the EMP Commission critique and direct a new assessment be prepared that supersedes the 2014 JAEIC EMP report.*

APPENDIX A Legislation Re-establishing the Commission

SEC. 1089. REESTABLISHMENT OF COMMISSION TO ASSESS THE THREAT TO THE UNITED STATES FROM ELECTROMAGNETIC PULSE ATTACK.

(a) REESTABLISHMENT.—The commission established pursuant to title XIV of the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 (as enacted into law by Public Law 106–398; 114 Stat. 1654A–345), and reestablished pursuant to section 1052 of the National Defense Authorization Act for Fiscal Year 2006 (Public Law 109–163; 50 U.S.C. 2301 note), known as the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack, is hereby reestablished.

(b) MEMBERSHIP.—Service on the Commission is voluntary, and Commissioners may elect to terminate their service on the Commission. If a Commissioner is unwilling or unable to serve on the Commission, the Secretary of Defense, in consultation with the chairmen and ranking members of the Committees on Armed Services of the House of Representatives and the Senate, shall appoint a new member to fill that vacancy.

(c) COMMISSION CHARTER DEFINED.—In this section, the term "Commission charter" means title XIV of the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 (as enacted into law by Public Law 106–398; 114 Stat. 1654A–345 et seq.), as amended by section 1052 of the National Defense Authorization Act for Fiscal Year 2006 (Public Law 109–163; 50 U.S.C. 2301 note) and section 1073 of the John Warner National Defense Act for Fiscal Year 2007 (Public Law 109–364; 120 Stat. 2403).

(d) EXPANDED PURPOSE.—Section 1401(b) of the Commission charter (114 Stat. 1654A–345) is amended by inserting before the period at the end the following: ", from non-nuclear EMP weapons, from natural EMP generated by geomagnetic storms, and from proposed uses in the military doctrines of potential adversaries of using EMP weapons in combination with other attack vectors.".

(e) DUTIES OF COMMISSION.—Section 1402 of the Commission charter (114 Stat. 1654A–346) is amended to read as follows:

"SEC. 1402. DUTIES OF COMMISSION.

"The Commission shall assess the following:

"(1) The vulnerability of electric-dependent military systems in the United States to a manmade or natural EMP event, giving special attention to the progress made by the Department of Defense, other Government departments and agencies of the United States, and entities of the private sector in taking steps to protect such systems from such an event.

"(2) The evolving current and future threat from state and non-state actors of a manmade EMP attack employing nuclear or non-nuclear weapons.

"(3) New technologies, operational procedures, and contingency planning that can protect electronics and military systems from the effects a manmade or natural EMP event.

"(4) Among the States, if State grids are protected against manmade or natural EMP, which States should receive highest priority for protecting critical defense assets.

"(5) The degree to which vulnerabilities of critical infrastructure systems create cascading vulnerabilities for military systems.".

(f) REPORT.—Section 1403 of the Commission charter (114 Stat. 1654A–345) is amended by striking "September 30, 2007" and inserting "June 30, 2017".

(g) TERMINATION.—Section 1049 of the Commission charter (114 Stat. 1654A–348) is amended by inserting before the period at the end the following: ", as amended by the National Defense Authorization Act for Fiscal Year 2016".

APPENDIX B High Altitude Nuclear Explosion-Generated Electromagnetic Effects

In the case of high altitude nuclear bursts, three main phenomena come into play, each with distinct associated system effects:

1. The first, a "prompt" EMP field, also referred to as E1, is created by gamma ray interaction with stratospheric air molecules. It peaks at tens of kilovolts per meter in a few nanoseconds, and lasts for a few hundred nanoseconds. E1's broad-band power spectrum (frequency content in the 10s to 100s of megahertz) enables it to couple to electrical and electronic systems in general, regardless of the length of their penetrating cables and antenna lines. Induced currents range into the 1000s of amperes. Exposed systems may be upset or permanently damaged.
2. The second component of the EMP field, referred to as E2, is produced by delayed gamma rays and neutron-induced currents, lasts from microseconds to milliseconds, and has a magnitude in the hundreds of volts per meter. Its spectral characteristics are similar to those of naturally occurring lightning.
3. The third component, late-time EMP, also referred to as magnetohydrodynamic (MHD) EMP or E3, is caused by the distortion of the earth's magnetic field lines due to the expanding nuclear fireball and rising of heated and ionized layers of the ionosphere. The change of the magnetic field at the earth's surface induces currents of 100s-1000s of amperes in long conducting lines (a few kilometers or greater) that damage components of the electric power grid itself as well as connected systems. Long-line communication systems are also affected, including copper as well as fiber-optic lines with repeaters. Transoceanic cables are a prime example of the latter.

Solar storm geomagnetic disturbance (GMD) effects are the result of large excursions in the flux levels of charged particles from the Sun and their interactions with the Earth's magnetic field and upper atmosphere. Perturbation of the Earth's magnetic field, similar to MHD EMP, can generate overvoltages in long-line systems over large regions of the earth's surface affecting electric power and communication transmission networks.

For each effect, directly-affected systems may be upset or permanently damaged. For unmanned systems and industrial control systems, upset effects can cascade to cause permanent damage to other connected systems. Wide-area electromagnetic system effects are challenging due to their near-simultaneous initial effects and cascading effects on a wide array of infrastructures. Infrastructure systems comprised of long-line conductor networks are the most vulnerable to both effects. Susceptible networks include the electric power grid, land-line communications, and interstate pipelines. Effects on these networks will cascade to most other

infrastructures. Smaller, self-contained, self-powered infrastructure systems (e.g. hand-held radios and vehicles) are also directly vulnerable, but only to EMP (not GMD) and to a lesser degree than long-line networks.

BIOGRAPHIES

COMMISSIONERS

Dr. William R. Graham is Chairman of the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack. He was 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. Previously he served as a member of several high-level study groups, including the Department of Defense Transformation Study Group, the Defense Science Board, the Commission to Assess United States National Security Space Management and Organization (the Rumsfeld Commission on Space), the Commission to Assess the Ballistic Missile Threat to the United States (also led by Hon. Donald Rumsfeld), and the National Academies' Board on Army Science and Technology. 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. Before going to the White House, he served as the Deputy Administrator of NASA. For 11 years, he served as a member of the Board of Directors of the Watkins-Johnson Company.

Dr. John S. Foster, Jr. began his career at the Radio Research Laboratory of Harvard University in 1942 and then volunteered to be an advisor to the 15th Army Air Force on radar countermeasures in Italy. In 1952, Dr. Foster joined the Lawrence Livermore National Laboratory, designed nuclear weapons, became Director of that Laboratory, then in 1965 served as Director of Defense Research and Engineering for the Department of Defense until 1973. He joined TRW to work on energy programs and then served on the Board, retiring in 1988. He currently serves as a consultant to LLNL and an Advisor to STRATCOM SAG Panel. He has served on the Air Force Scientific Advisory Board, Army Scientific Advisory Panel, Ballistic Missile Defense Advisory Committee, and Advanced Research Projects Agency. From 1973 – 1990 he was a member of the President's Foreign Intelligence Advisory Panel. He served as Chairman of the Defense Science Board from 1990 to 1993. He served on the Congressional Commission on the Strategic Posture of the United States and on the Advisory Committee to the Director of DARPA.

Mr. Earl Gjelde, P.E., 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 (19801982). 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 served as Vice President for Corporate Development at SAIC, where he was the company's leading cyberspace security advisor to the President's National Security Telecommunications Advisory Committee (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 has been 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).

Gen Richard L. Lawson, USAF (Ret.), served as Chairman of Energy, Environment and Security Group, Ltd., and as President and CEO of the National Mining Association. He also served 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; Commander, 8th Air Force; 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 served as the 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 has also provided 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 retired from a career-long position on the technical staff of Lawrence Livermore National Laboratory, operated by the University of California for the U.S. Department of Energy, and an extended term as a Research Fellow of the Hoover Institution at Stanford University. Since his retirement a decade ago, Dr. Wood has continued part-time technical consulting in the commercial sector and serving as an External Advisor of the Bill & Melinda Gates Foundation, the world's largest private charity, focusing his efforts on global health and development. Dr. Wood holds the distinction of being the most inventive American in history, holding more U.S. patents on new inventions than any other person, including Thomas Edison, the previous record-holder.

Dr. Joan Woodard was Executive Vice President and Deputy Director of Sandia National Laboratories, responsible for all of Sandia's programs, operations, staff, and facilities. She was also responsible for the laboratory's strategic planning. Previously, 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 percent of the programs included industrial or academic partners, and the nature of the work ranged from basic research to prototype systems evaluation.

SENIOR ADVISORS

Dr. George H. Baker is a Professor Emeritus at James Madison University, where he directed the JMU Institute for Infrastructure and Information Assurance. Previously, Dr. Baker led the Defense Nuclear Agency's Electromagnetic Pulse (EMP) program, directed the Defense Threat Reduction Agency's assessment arm, and served as a member of the Congressional EMP

Commission Staff. Dr. Baker holds an M.S. in Physics from University of Virginia, and a Ph.D. in Engineering Physics from the U.S. Air Force Institute of Technology. Currently, Dr. Baker is CEO of BAYCOR, LLC, and is Director of the Foundation for Resilient Societies.

Mr. William R. Harris is an international lawyer specializing in arms control, nuclear non-proliferation, energy policy, and continuity of government. He worked on Hot Line upgrades, creation of linked Nuclear Risk Reduction Centers, and was a co-drafter of arms limitation treaties in 1986-87, 1991, and 1993. Mr. Harris worked for the RAND Corporation and in a variety of assignments for the U.S. Government. Mr. Harris holds a B.A. from Harvard College and a J.D. from Harvard Law School. Mr. Harris serves as Secretary and attorney for the Foundation for Resilient Societies.

Dr. Peter Vincent Pry is a recognized expert on protection strategies for electromagnetic pulse (EMP) and related threats. In addition to his service for the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, he has served on the Congressional Strategic Posture Commission, as Executive Director of the U.S. Nuclear Strategy Forum and the Task Force on National and Homeland Security (both Congressional Advisory Boards); as Professional Staff on the House Armed Services Committee of the U.S. Congress, with portfolios in nuclear strategy, WMD, Russia, China, NATO, the Middle East, intelligence, and terrorism; as an Intelligence Officer with the Central Intelligence Agency; and as a Verification Analyst at the U.S. Arms Control and Disarmament Agency. Dr. Pry has written numerous books and articles on national security issues.

Dr. William A. Radasky is President and Managing Engineer at the Metatech Corporation. Metatech develops technically sound and innovative solutions to problems in all areas of electromagnetic environmental effects, including: electromagnetic interference and compatibility, geomagnetic storm assessments and protection, nuclear electromagnetic pulse prediction, assessments, protection and standardization, and intentional electromagnetic interference assessments, protection and standardization. Dr. Radasky has published over 400 technical papers, reports and articles dealing with electromagnetic interference (EMI) and protection. In 2004 he received the Lord Kelvin Award from the International Electrotechnical Commission for exceptional contributions to international standardization.

Dr. David Stoudt is a Senior Executive Advisor at Booz Allen where he provides leadership and guidance on the science and business of advancing directed energy capabilities for American warfighters. He previously spent 32 years serving in the Department of Navy, with deep experience in directed energy and electric weapon systems, including high-energy lasers, the electromagnetic rail gun, and high-power microwave weapon systems. Among other honors, David has received multiple Meritorious Civilian Service Awards, the Navy Distinguished and Superior Civilian Service Awards, and the Naval Sea Systems Command Scientist of the Year Award.

Ambassador R. James Woolsey Jr., J.D., is a national security and energy specialist and former Director of Central Intelligence who headed the Central Intelligence Agency from

February 5, 1993, until January 10, 1995. A lawyer by training and trade, he held a variety of government positions in the 1970s and 1980s, including as Under Secretary of the Navy from 1977 to 1979, and was involved in treaty negotiations with the Soviet Union for five years in the 1980s, including as Chief Negotiator of the Conventional Forces in Europe Treaty.

COMMISSION REPORTS

REPORTS OF THE COMMISSION

Executive Report, 2004

Critical National Infrastructures Report, 2008

Assessing the Threat from EMP Attack: Executive Report, 2017

Recommended E3 HEMP Heave Electric Field Waveform for the Critical Infrastructures, 2017

Assessment of the 2014 JAEIC Report on High-altitude Electromagnetic Pulse (HEMP) Threats, **SECRET//RD-CNWDI//NOFORN**, 2017

STAFF PAPERS TO THE COMMISSION

G. Baker. Risk-Based National Infrastructure Protection Priorities for EMP and Solar Storms, 2017

W.R. Graham. Chairman's Report, 2017.

J. G. Kappenman and W.A. Radasky. Examination of NERC GMD Standards and Validation of Ground Models and Geo-Electric Fields, 2017

T.S. Popik, G.H. Baker, and W.R. Harris. Electric Reliability Standards for Solar Geomagnetic Disturbances, 2017

P.V. Pry. Nuclear EMP Attack Scenarios and Combined-arms Cyber Warfare, 2017

P.V. Pry. Political-Military Motives for Electromagnetic Pulse Attack, 2017

P.V. Pry. Foreign Views of Electromagnetic Pulse Attack, 2017

P.V. Pry. Life without Electricity: Storm Induced Blackouts and Implications for Electromagnetic Pulse Attack, 2017

P.V. Pry. Nuclear Terrorism and Electromagnetic Pulse Attack, 2017

E. Savage and W. Radasky. Late-Time (E3) HEMP Heave Parameter Study, **SECRET//RD**, 2017