

Statement for the Record

Brandon Wales
National Protection and Programs Directorate
Department of Homeland Security

Before the
House Committee on Homeland Security
United States House of Representatives
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

September 12, 2012

Thank you, Chairman Lungren, Ranking Member Clarke, and distinguished Members of the Committee. It is a pleasure to appear before you today to discuss the nature of the threat posed by electromagnetic pulse (EMP) to our Nation and its critical infrastructure, including its cyber, communications, and electric-grid assets, as well as to discuss the Department of Homeland Security's (DHS) preparations to respond to and recover from potential EMP attacks.

Over the past several decades, the threat to digital and physical infrastructures has grown. For example, today's power grid and information networks are much more vulnerable to EMP than those of a few decades ago.¹ The Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack recommended in its final report that DHS "play a leading role in spreading knowledge of the nature of prudent mitigation preparations for EMP attack to mitigate its consequences."² The Department takes that recommendation seriously and welcomes in cooperation with other government agencies increasing understanding of this critical topic.

Background

An EMP is the burst of electromagnetic radiation created when a nuclear weapon is detonated or when a non-nuclear EMP weapon is used. Naturally occurring solar weather can generate effects similar to one component of an EMP. EMPs can be high frequency, similar to a flash of lightning or a spark of static electricity, or low frequency, similar to an aurora-induced

¹ Since the 1980s, our power grid control systems and information infrastructures have been growing in their reliance on the Ethernet and computers, which are much more vulnerable to E1 EMP than previous control and communications systems designs. Likewise, the power grid today is much more vulnerable to (E3 EMP) and solar storms than the grid of the 1970s and 80s due to the increasing network size and evolution to higher operating voltages.

² "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures," April 2008, page 181. This report presents the results of the Commission's assessment of the effects of a high altitude EMP attack on our critical national infrastructures and provides recommendations for their mitigation.

phenomenon.³ An EMP can spike in less than a nanosecond or can continue longer than 24 hours, depending on its source. The consequences of an EMP range from permanent physical damage to temporary system disruptions and can result in fires, electric shocks to people and equipment, and critical service outages. There are four general classes of EMP.

High altitude EMP (HEMP) results from a nuclear detonation typically occurring 15 or more miles above the Earth's surface. The extent of HEMP effects depends on several factors, including the altitude of the detonation, the weapon yield and design, and the electromagnetic shielding, or "hardening," of assets. One high-altitude burst could blanket the entire continental United States and could cause widespread power outages and communications disruptions and possible damage to the electricity grid for weeks or longer.⁴ HEMP threat vectors can originate from a missile, such as a sea-launched ballistic missile; a satellite asset; or a relatively low-cost balloon-borne vehicle. A concern is the growing number of nation-states that in the past have sponsored terrorism and are now developing capabilities that could be used in a HEMP attack.

Source Region EMP (SREMP) is a burst of energy similar to HEMP but differs in that it is created when a nuclear weapon detonates at lower altitudes within the atmosphere. SREMP can occur when a detonation occurs on or near the ground, as would likely be the case of a terrorist nuclear device attack. A SREMP's electromagnetic field is much more limited in range than that from HEMP; it would only affect a delimited geographic area. SREMP can induce very high currents on power cables or metallic communications lines near the fireball, and it can send extreme spikes of energy great distances from the blast zone along these metal lines, potentially causing fires where these lines meet other infrastructures. In addition, the SREMP travels through the air and can damage or disrupt equipment connected to Ethernet cables, telephone lines, and power cords out to 70 miles or more. Electronic systems not connected to power cords or communications lines, such as a cell phone, are generally resistant to SREMP but become useless if the infrastructure that supports them is non-functional. While SREMP is not the primary reason a terrorist would detonate a nuclear weapon, it is important to note that all ground-based detonations create SREMP of sufficient magnitude to cause infrastructure disruptions, including an improvised nuclear device, a crude nuclear device that could be built from the components of a stolen weapon or from using nuclear materials. Given the possible impacts of SREMP, such as secondary fires and the disruptions of power, communications, and other

³ Aurora-induced phenomena refer to effects like geomagnetically-induced currents in the power grid that are caused by solar storms which are associated with increased aurora activity. Although there are many different phenomena associated with solar storms, one of the most important is the geomagnetically-induced quasi-dc current flow that can damage our power transmission networks.

⁴ "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures," April 2008, page vi, "When a nuclear explosion occurs at high altitude, the EMP signal it produces will cover the wide geographic region within the line of sight of the detonation. This broad band, high amplitude EMP, when coupled into sensitive electronics, has the capability to produce widespread and long lasting disruption and damage to the critical infrastructures that underpin the fabric of U.S. society." See also: Glasstone, S., P.J. Dolan, "The Effects of Nuclear Weapons," Chapter XI on EMP, U.S. Dept. of Energy, 1977

critical infrastructures, it is an important consideration in our Department's planning to mitigate and respond to this type of attack.

Unlike HEMP and SREMP, which primarily disrupt Earth-based infrastructures, System Generated EMP (SGEMP) is a threat to space-based assets, such as satellites or a space station. SGEMPs originate from a nuclear weapon detonation above the atmosphere that sends out damaging X-rays that strike space systems. Both SGEMP and HEMP are similar, in that they both originate from a high-altitude burst. The Department's chief concern with SGEMP and other related high-altitude nuclear effects is that satellite or other space systems that support critical communications and navigation services, as well as essential intelligence functions, can be immediately disrupted. SGEMP and other related effects could also harm systems supporting any astronaut in space.

The fourth type of EMP is Non-Nuclear EMP, or NNEP. This type of EMP can be created by Radio Frequency Weapons (RFWs), devices designed to produce sufficient electromagnetic energy to burn out or disrupt electronic components, systems, and networks. RFWs can either be electrically-driven, where they create narrowband or wideband microwaves, or they can be explosively driven, where an explosive is used to compress a magnetic field to generate the pulse. Multiple nations have used RFWs since the 1960s to disable or jam security, communications, and navigation systems; induce fires; and disrupt financial infrastructures. Devices that can be used as RFWs have unintentionally caused aircraft crashes and near crashes, pipeline explosions, gas spills, computer damage, vehicle malfunctions, weapons explosions, and public water system malfunctions.⁵ The Department believes that much of the mitigation and planning we are doing for other types of EMP will help reduce our threat to NNEP.

Solar Weather

Solar Weather is created as a result of massive explosions on the sun that may shoot radiation towards the Earth. These effects can reach the Earth in as little as eight minutes with Solar Flare X-rays or over 14 hours later with a Coronal Mass Ejection (CME) plasma hurricane. An extreme CME is the Department's biggest Solar Weather concern. It could create low-frequency EMP similar to a megaton-class nuclear HEMP detonation over the United States, which could disrupt or damage the power grid, undersea cables, and other critical infrastructures. The United States experiences many solar weather events each year, but major storms that could significantly impact today's infrastructures are not common but have previously occurred in 1921 and 1859 and possibly in several other years prior to the establishment of the modern

⁵ Robert L. Schweitzer, LTG (ret) USA, "Radio Frequency Weapons: The Emerging Threat and Policy Implications," Eagan, McAllister Associates, October 1998; see also: Overview of Evolving and Enduring Threats to Information Systems, National Communications System, August 2012.

power grid. The U.S. Department of Energy and utility owners and operators have been focusing on potential threats and steps that utilities can take to reduce possible impacts.⁶ Work is underway in cooperation with a number of federal agencies including the: National Aeronautics and Space Administration (NASA), Nation Oceanic and Atmospheric Administration (NOAA), United States Geological Survey, Department of Energy, Department of Defense, and DHS with industry support and participation to ensure this threat is understood.

Potential Impacts to Critical Infrastructure

Overall, EMP in its various forms can cause widespread disruption and serious damage to electronic devices and networks, including those upon which many critical infrastructures rely, such as communication systems, information technology equipment, and supervisory control and data acquisition (SCADA) modules. SCADA modules are used in infrastructure such as electric grids, water supplies, and pipelines. The disruptions to SCADA systems that could result from EMP range from SCADA control errors to actual SCADA equipment destruction. Secondary effects of EMP may harm people through induced fires, electric shocks, and disruptions of transportation and critical support systems, such as those at hospitals or sites like nuclear power plants and chemical facilities.

EMP places all critical infrastructure sectors at risk. Those sectors that rely heavily on communications technology, information technology, the electric grid, or that use a SCADA system are particularly vulnerable. The complex interconnectivity among critical infrastructure sectors means that EMP incidents that affect a single sector will likely affect other sectors – potentially resulting in cascading failures. The interdependent nature of all 18 critical infrastructure sectors complicates the impact of the event and recovery from it.

DHS's Efforts to Study, Mitigate, and Respond to EMP Attacks

The Department, acting through the Federal Emergency Management Agency (FEMA), the National Protection and Programs Directorate (NPPD) and the Science and Technology Directorate (S&T), has worked extensively to help recognize EMP as a threat to the Nation. Specifically, the Department is working collaboratively, both internally and with external stakeholders, in various arenas to reduce risk. For example, DHS has exercised scenarios involving both EMP and solar weather and is developing plans to help address these evolving threats. Likewise, FEMA and other government agencies are working with states and industry. For example, FEMA is deploying new capabilities as part of the Integrated Public Alert and Warning System, such as the protected Emergency Alert System Primary Entry Point AM and

⁶ In the last 200 years, only the 1859 and 1921 solar superstorms are believed by experts to have exceeded the 4,000 nanoTesla/minute level over the U.S. If one of these storms were to occur today, many experts believe they would likely damage key elements of the power grid and could cause very long-term power outages over much of the United States.

FM radio stations that would be used by the President and key leadership to help keep the public informed and alerted during a major EMP event.⁷ Both NASA and NOAA are improving and testing their Space Weather warning systems. Many of the Federal Government's missions rely on satellite imagery, communications satellites, and GPS for their execution. The potential impact of solar storms on satellites led Secretary Napolitano to issue the DHS Space Policy on February 3, 2011, which committed the Department to working with both private and public sector partners on increasing the resilience of mission essential functions.

Two offices within NPPD are at the forefront of understanding and working to identify how EMP can impact the homeland security enterprise. First, the Office of Cybersecurity and Communications (CS&C) has worked extensively to model and assess EMP effects and conduct research and propose solutions to understand and mitigate EMP risks. As a result, CS&C has produced many assessments of the risks and mitigation options related to EMP. In particular, significant progress has been made in the last few years in modeling and understanding the risks of SREMP associated with an improvised nuclear device.

NPPD's Office of Infrastructure Protection (IP) also plays a significant role in the Department's work on EMP. IP conducted a study in 2010 on EMP's potential impact on extra high voltage (EHV) transformers for the Western United States' electrical grid. The study included findings about EMP from both artificial and naturally occurring incidents and recommended options for hardening EHV transformers from EMP.

S&T has led much of the Department's research in the EMP area and is conducting important work through the Recovery Transformer (RecX) Project to increase the resiliency of the EHV transmission power grid, through the use of more mobile and modular transformers. EHV transformers are very large, extremely difficult to transport, and until 2009 primarily manufactured overseas, complicating rapid recovery and restoration efforts. This effort has developed a prototype EHV transformer that can quickly be deployed to a site, via a series of trailers and semi-trucks, and then installed, assembled, and energized rapidly. The prototype RecX was demonstrated and installed in the grid at a host utility and is currently undergoing a one-year observational period to verify its performance.

Another Departmental effort to increase the resiliency of the power grid is the S&T Resilient Electric Grid Project. S&T has developed a power-surge limiting, high temperature, superconducting cable for electric grid resiliency that enables distribution-level substations to interconnect and share power and assets, while helping electric utilities manage power surges arising from a variety of causes that can cause cascading blackouts and permanent damage to electrical equipment. The interconnection of substations increases the resiliency of the grid by creating multiple paths for power flow. Superconducting cables also provide additional benefits

⁷ To date, 17 national level Emergency Alert System radio stations have been protected against EMP. Within the next year, another 20 national level EAS radio stations are planned to have EMP protection installed.

such as allowing more power to flow through a smaller cable with lower transmission losses. The cable will be installed for testing and evaluation in Yonkers, NY, in 2014. Several approaches to improving the resiliency of the electrical grid are underway both in the United States and abroad that hold promise to reduce the vulnerability of extra large transformers and reduce the threat to the electricity grid.

Conclusion

DHS has pursued a deeper understanding of the EMP threat as well as its potential impacts, effective mitigation strategies, and a greater level of public awareness and readiness in cooperation with other Federal agencies and private equipment and system owners and operators through various communications channels. However, more work is needed to understand the risk posed by EMP and solar weather to all sectors, through direct and cascading impacts. I commend the Committee for its interest in this key issue and look forward to your questions.