Electromagnetic Pulses (EMPs): *Myths vs. Facts*

This document provides factual responses to unsupported or inaccurate claims about the electric sector's preparedness to deal with electromagnetic pulses, or EMPs, that may impact the electric power grid.

Myth: All magnetic interference is the same.

Fact: There are important differences between intentional, manmade magnetic disturbances or electromagnetic pulses (EMPs), such as those from directed energy weapons or nuclear blasts, and naturally occurring geomagnetic disturbances (GMDs), such as solar flares. Given these differences, each type of threat needs to be assessed and addressed independently, with appropriate mitigation and protection strategies implemented for each.

- High-Altitude Nuclear Blast EMP: A high-level EMP caused by the detonation of a nuclear weapon in the atmosphere is a high-consequence, low-likelihood threat that would have a potentially catastrophic impact on society. Further, since the planning and launching of a nuclear attack on U.S. critical infrastructure would be an act of war or terrorism, the federal government must be primarily responsible for preventing high-level EMPs as a matter of national security. The impacts of a high-level EMP on the electric grid are still not fully understood, but are being studied by the Electric Power Research Institute, the federal national labs, and others, with some mitigation strategies, such as shielding equipment and procuring spare equipment, already being utilized.

- Directed Energy EMP Weapons: This category of devices may pose a more narrowly focused EMP threat to a single facility or piece of equipment similar to a traditional physical attack. Thus, mitigation strategies include more typical physical protection measures such as line-of-site security, access controls, and system redundancy.

- Solar Flare GMDs: GMDs caused by solar flares are naturally occurring events the electric industry has addressed for decades. They result in two types of risks: (1) damage to bulk power system assets (e.g., transformers); and (2) loss of reactive power support, which could lead to voltage instability and power system collapse. Based on these risks, the North American Electric Reliability Corporation (NERC) has developed mandatory and enforceable GMD industry standards that are on track for implementation and further refinement.

Myth: Utilities are self-regulated for reliability and security at the federal level.

Fact: Pursuant to the Energy Policy Act of 2005, all electric utilities are subject to mandatory reliability standards, including standards addressing GMDs, cybersecurity, and physical security. These standards are developed and enforced by NERC and approved by the Federal Energy Regulatory Commission (FERC). NERC is an independent, American National Standards Institute-certified, standards-setting body. FERC also has independent authority to enforce the mandatory reliability standards and to order NERC to develop new standards.

The NERC standards process is open and transparent, and leverages the experience of industry experts. NERC's independent Board also has the authority to approve or request that drafting teams

develop a specific standard. Additionally, FERC can, and has, required NERC to develop standards to address specific issues, including the GMD and physical security standards.

Myth: The electric power industry is not responsive to threats such as EMP and GMD.

Fact: NERC has developed mandatory and enforceable reliability standards to help protect the grid from the impacts of GMDs. Ongoing technical assessments of these threats continue to adequately define their scope and magnitude so that the electric sector can respond with sensible and effective mitigation measures as part of its overall risk management strategy.

FERC approved the first phase of the GMD standards in June 2014, and they will become enforceable on April 1, 2015. NERC filed the second-phase GMD standards with FERC in January 2015. FERC is expected to issue a notice of proposed rulemaking to approve the standard in the spring of 2015.

While standards ensure that every electric utility meets a baseline level of security, the electric industry also relies on close coordination and partnerships with law enforcement and security agencies of the federal government to help defend against hostile nation-states or attacks against the United States, especially in the case of nuclear threats from an EMP device.

Myth: It would cost only $2 billion to protect the entire grid from any EMP attack.

Fact: Some EMP advocates claim that, based on a 2008 report of the Congressional EMP Commission, it would cost only $2 billion to protect the national electric grid against EMP threats. However, the EMP Commission report does not directly state such costs, nor do several members of the EMP commission agree with that claim.

One leading EMP advocate who cites the $2 billion figure has suggested that $2 billion would cover only the cost to protect transformers, with an additional $20 billion needed to protect the entire electric grid. And, a former Department of Defense official familiar with EMP threats and the Commission report has testified the $2 billion figure could be "off by a factor of ten or more." Thus, cost estimates to protect the grid have not been shown to be reliable or accurate.

The debate over the cost to protect the electric grid from EMPs also ignores the reality that other sectors of the economy likely will be affected by a nuclear EMP attack, including other critical infrastructure sectors upon which the electric sector depends to generate or distribute electricity. It makes little sense to protect the electric grid while ignoring these other critical infrastructure sectors.

Myth: There are quick, easy, and low-cost solutions, such as blocking devices, to protect the electric grid from all threats.

Fact: Many EMP mitigation techniques remain unproven and are potentially more expensive than claimed by their promoters, many of whom stand to benefit from their deployment. Further, placing blocking devices on the grid could have unintended consequences for an event that is relatively unlikely to happen. For instance, some mitigation measures to prevent damage from an EMP could actually reduce the effectiveness of measures to address GMDs, which occur much more frequently.

The best risk mitigation for an EMP event, especially one as severe as a high-altitude nuclear explosion, is prevention. The prevention or preemption of such attacks is within the purview of the nation's law enforcement, military, and intelligence functions.

Myth: An EMP event that would take down the grid is "easy to perpetrate."

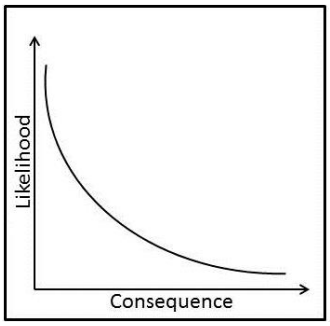
Fact: This is false. To fully understand the likelihood, we must again understand the threats.

Directed Energy Weapon: To cause significant damage to the grid, dozens of directed energy weapons would need to be built, deployed, and detonated in a coordinated attack across the country—without being detected or stopped by law enforcement first. While not impossible, such a strategy is significantly more complicated to plan and carry out than claimed.

High-Altitude Nuclear Explosion: The list of adversaries with this capability is significantly smaller and well-known, and the material required to produce and launch such a device is highly monitored by U.S. intelligence authorities and international organizations. Again, the prevention of such attacks is the responsibility of the nation's military and intelligence agencies.

Myth: Electric utilities are completely unprepared for an EMP event.

Fact: Electric utilities plan for a number of threats to the grid. As they make their risk-based threat assessments, they identify the likelihood and consequence of each threat to understand their security priorities.



Solar storms, some of which can cause GMD events, are naturally occurring phenomena that come with some prior warning. Utility system owners and operators recognize the risks posed by solar storms and have put into place operating processes and procedures to manage GMD risks.

The high-altitude nuclear weapon scenario is noteworthy because its consequences could be extraordinarily high; however, given U.S. military and intelligence community capabilities, as well as geo-political deterrence efforts, the relative likelihood of such an attack is very low. Additionally, with strategic EMP shielding, spare equipment stockpiles, and partnerships with government, the electric utility industry already is taking preparatory steps to respond and recover. Still, in the case of potentially high-consequence, low-likelihood events like a nuclear attack, the most effective mitigation strategy is deterrence, prevention, or preemption by military means.

The use of a directed energy weapon may be statistically more likely, but the consequence is much less because it would be a localized event. In addition, with 45,000 substations across the United States, the destruction of one or two substations would not have a widespread impact on the grid. A larger coordinated attack could have a potentially broader impact, but is less likely to occur because such coordinated plots have a higher chance of detection and intervention by law enforcement and intelligence agencies.

Myth: Electric utilities don't take threats to their infrastructure seriously.

Fact: Protecting the nation's electric power grid and ensuring a reliable and affordable supply of energy are top priorities for the electric power industry. Electric utilities take all threats to the grid seriously, whether they are natural disasters or man-made threats.

Electric utilities also have every incentive to protect their systems: first, there is a public service responsibility to maintain reliable and affordable electricity service; second, there is an economic

incentive to keep the lights on. To help keep electricity reliable and affordable, utilities and state regulators assess each type of threat to grid security as part of an overall risk management strategy.

Myth: The industry has done very little continuity planning for hard-to-replace equipment such as large power transformers.

Fact: The electric power industry has taken specific steps to prepare for, prevent, respond to, and recover from threats to the electric grid. Electric utilities plan for all types of contingencies and have spare equipment available as part of their business continuity planning. Just as utilities share emergency restoration crews as part of the industry's voluntary mutual assistance program, they also share transformers and other equipment regularly.

Recognizing that catastrophic destruction of a significant substation can potentially cause substantial power loss, the electric power industry created the Spare Transformer Equipment Program (STEP) in 2006. More than 50 electric utilities dispersed across the country and engaged in bulk power transmission services are members of STEP, and this number continues to grow.

STEP is designed to ensure that the electric power industry has a process in place to have sufficient spare transformer capacity available. Since there is interchangeability between transformers within a voltage class, STEP provides a ready mechanism for participating electric utilities to share assets in the event of catastrophic destruction.

To complement STEP, *SpareConnect* provides an online tool for electric utilities, asset owners, and operators to network with other *SpareConnect* members concerning sharing of transmission and generation step-up transformers and related equipment, including bushings, fans, and auxiliary components. *SpareConnect* establishes a digital, formal, secure, and efficient program to rapidly communicate equipment needs in the event of an emergency or of other non-routine failures.

Myth: Regardless of cost, we must immediately make all necessary investments to protect the electric grid from an EMP.

Fact: Deploying expensive technology that is unproven is not effective risk management.

The electric power sector often is described as the most critical of the critical infrastructure sectors. While it is true that other critical sectors depend on a reliable supply of electricity for their operations, the electric power industry likewise is dependent on other critical infrastructure sectors for business continuity as well. Electric utilities need: water to cool their systems and to create steam that spins generating equipment; telecommunications to operate the grid; and transportation and pipeline systems to move the fuel sources they use. Thus, our adversaries don't have to just attack the electric grid to disrupt power.

It takes a coordinated effort among different critical infrastructure sectors and the government to protect grid reliability and operations. In the case of a high-level EMP event that could potentially render any device containing a microprocessor inoperable, the issue should be addressed across all critical sectors by national defense authorities. Again, the best strategy to protect against such EMP events is to prevent them from occurring in the first place.

Myth: Industry and government are not adequately sharing information in order to ensure grid security.

Fact: The electric power industry already engages in many information-sharing efforts involving government and the private sector, and is considered a model sector in this area. Of course, more information sharing is needed, which is why the electric power industry supports passage of information-sharing legislation, along with liability protection for those who engage in information sharing with the federal government. In addition to close coordination and information sharing among electric utilities, the industry partners with federal agencies, including the Department of Homeland Security, the Department of Energy, and FERC, to improve sector-wide resilience against all hazards and potential threats.

Currently, there are several existing industry-government information-sharing mechanisms:

- **The Electricity Sector Information Sharing and Analysis Center (ES-ISAC):** The ES-ISAC gathers industry information on security-related events for sharing with its government partners and shares government information on threats with industry.
- Working with the government, the industry has formed the **Electricity Subsector Coordinating Council (ESCC)** to serve as the principal liaison between the federal government and the electric power sector. The ESCC brings senior utility executives together with senior Administration officials from the White House, several Cabinet agencies, federal law enforcement, and national security organizations.

  This high-level coordination has supported the rapid deployment of tools used to help detect security threats; improved preparation by exercising coordinated responses to attacks on the grid; and has helped to make sure that information about threats is communicated quickly among government and industry stakeholders. Additionally, the ESCC is focusing on technology transfers from the government to utilities, allowing the industry to benefit from the research and development that the national labs and the military have done to protect infrastructure systems.
- DHS's **National Cybersecurity and Communications Integration Center (NCCIC)** works with federal, state, and local governments; intelligence and law enforcement communities; and the private sector to prepare for, assess, and respond to cyber events that might impact the electric power sector.