

STRATEGY
FOR
PROTECTING AND PREPARING THE HOMELAND AGAINST THREATS OF ELECTROMAGNETIC PULSE
AND
GEOMAGNETIC DISTURBANCES

October 9, 2018

Vision: *The United States is prepared for extreme electromagnetic incidents and capable of quickly restoring critical infrastructure and supporting communities to fully recover.*

Table of Contents

Introduction **3**
Mandate and Scope 4
Background 5
Strategy Summary 6
Implementation 7
Acknowledgments 8
Goal 1: Improve Risk Awareness of Electromagnetic Threats and Hazards **10**
Goal 2: Enhance Capabilities to Protect Critical Infrastructure **13**
Goal 3: Promote Effective Electromagnetic-Incident Response and Recovery Efforts **16**
Appendices
Appendix A: Technical Background A-1

Introduction

Extreme electromagnetic incidents caused by an intentional electromagnetic pulse (EMP) attack or a naturally occurring geomagnetic disturbance (GMD, also referred to as "space weather") could damage significant portions of the Nation's critical infrastructure, including the electrical grid, communications equipment, water and wastewater systems, and transportation modes.[1] The impacts are likely to cascade, initially compromising one or more critical infrastructure sectors, spilling over into additional sectors, and expanding beyond the initial geographic regions.[2]

EMPs are associated with intentional attacks using high-altitude nuclear detonations, specialized conventional munitions, or non-nuclear directed energy devices. Effects vary in scale from highly local to regional to continental, depending upon the specific characteristics of the weapon and the attack profile. High-altitude electromagnetic pulse attacks (HEMP) using nuclear weapons are of most concern because they may permanently damage or disable large sections of the national electric grid and other critical infrastructure control systems.[3]

Similarly, extreme geomagnetic disturbances associated with solar coronal mass ejections (when plasma from the sun, with its embedded magnetic field, arrives at Earth) may cause widespread and long-lasting damage to electric power systems, satellites, electronic navigation systems, and undersea cables. Essentially, any electronics system that is not protected against extreme EMP or GMD events may be subject to either the direct "shock" of the blast itself or to the damage that is inflicted on the systems and controls upon which they are dependent.

For these reasons, the potential severity of both the direct and indirect impacts of an EMP or GMD incident compels our national attention. The Department of Homeland Security (DHS) has been actively analyzing the risk of the EMP-GMD problem set since its inception. The *Strategy for Protecting and Preparing the Homeland Against Threats of Electromagnetic Pulse and Geomagnetic Disturbances* (hereafter referred to as the "DHS Strategy") represents the Department's first articulation of a holistic, long-term, partnership-based approach to confronting this challenge. The DHS Strategy and the forthcoming companion Implementation Plan will improve the Department's understanding of electromagnetic threats and hazards and inform efforts

[1] See Appendix A: Technical Background for an expanded discussion of EMP, GMD, and their potential impacts.

[2] There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. Presidential Policy Directive 21 (PPD-21): "Critical Infrastructure Security and Resilience" identifies DHS as the lead for 10 critical infrastructure sectors including chemical, commercial facilities, communications, critical manufacturing , dams, emergency services, government facilities (with the General Services Administration), information technology, nuclear reactors, materials, and waste, and transportation systems (with the Department of Transportation). (See https://www.dhs.gov/critical-infrastructure-sectors).

[3] HEMP incidents are exo-atmospheric. Most EMP impacts from a nuclear blast *within* the atmosphere would be overtaken by the physical damage caused by pressure, heat, and radiation of the blast.

to increase national preparedness for any electromagnetic incident.[4,5] These documents will also guide Departmental management, oversight, and optimization of taxpayer resources.

The DHS Strategy development included engagement and collaboration across DHS Components and with interagency partners (including the Department of Energy (DOE), the Sector-Specific Agency (SAA) for the energy sector), as well as solicitation of input from the private sector through the Sector Coordinating Councils (SCC). Accordingly, development of the Implementation Plan will also include contributions from Federal partners and the private sector. The Implementation Plan will detail DHS roles and responsibilities, current and projected capabilities, timelines, and governance to effectuate the Strategy.[6]

Mandate and Scope

The Strategy has been developed pursuant to Section 1913 (a)(2)(A)(i) and (B)(i – v) of the *National Defense Authorization Act for Fiscal Year 2017* (FY 2017 NDAA), which directs DHS to provide a strategy that provides guidance and identifies key actions we must take as a Nation to protect and prepare the homeland against EMP attacks and naturally occurring GMD caused by solar activity.[7,8]

As established in the *Homeland Security Act of 2002*, as amended, DHS is responsible for recommending measures necessary to protect the critical infrastructure of the United States in partnership with Sector-Specific Agencies. DOE is the SSA for the energy sector and is responsible for ensuring the reliability of the national electric grid. The Department of Defense (DOD) is responsible for deterring and preventing foreign adversaries from using nuclear weapons against the United States as part of an EMP attack. Sector-specific responsibilities for space weather are given in the White House Executive Order 13744, *Coordinating Efforts to Prepare the Nation for Space Weather Events*, signed October 13, 2016.

The goals of the DHS Strategy address a full range of preparedness activities that reduce impacts from an electromagnetic event and ensure timely and effective reconstitution of affected areas to normal social and economic activity. The DHS Strategy and subsequent Implementation Plan incorporate the following elements as referenced by the FY 2017 NDAA requirement:

- Intelligence-based review, evaluation, and comparison of the risks and consequences of EMP and GMD to critical infrastructure;

---

[4] Definition of "Strategy" per *2017 DHS Strategic Planning Guidance*: Articulates the vision, goals, objectives, and outcomes that inform key budget, acquisition, and operational activities within the Department, specifying the current "problem," "why" the organization is particularly well-suited to address the problem, and "what" the organization needs to do to achieve the desired outcomes. A strategy does not direct specific operations and tactics, and in this sense is distinguished from an implementation plan, acquisition roadmap, or operational plan.

[5] Definition of "Implementation Plan" per *2017 DHS Strategic Planning Guidance*: Establishes the sequence of activities that the Department must perform for a strategy to succeed. An implementation plan identifies Department roles and responsibilities, current and anticipated capabilities, and any necessary resource considerations for each objective within the strategy's overarching goal and objective framework.

[6] Descriptions of DHS Component/Office roles and responsibilities will be delineated in the Strategy's implementation plan and will be linked to the Department's annual budget decision-making and review cycle.

[7] Additional requirements directed under FY 2017 NDAA Section 1913 (2)(A) to include an intelligence-based review and comparison of the risks and consequences of EMP and GMD were used to inform this strategy, but are classified and provided elsewhere. Requirements under FY 2017 NDAA Section 1913 (319) related to EMP and GMD mitigation research and development are incorporated into, and will be executed in, the implementation of this Strategy.

[8] As defined in Sec. 1913 of the FY 2017 NDAA, the term "EMP" means an electromagnetic pulse caused by a nuclear device or nonnuclear device, including such a pulse caused by an act of terrorism. The term "GMD" means a geomagnetic disturbance caused by a solar storm or another naturally occurring event.

- Findings of EMP-GMD research and development activities conducted by DHS, DOE National Labs, and other partners;
- Consultation with relevant Sector-Specific Agencies and Sector Coordinating Councils;
- Consideration of specific EMP-GMD threats and hazards to the electrical grid;
- Determination of critical utilities and national security assets that are at risk from extreme EMP and GMD incidents;
- Evaluation of emergency planning and response technologies that would address the findings and recommendations of EMP and GMD subject-matter experts;
- Review of the feasibility of rapidly isolating one or more portions of the electrical grid;
- Analysis of technology options that are available to improve the resiliency of critical infrastructure threats from EMP and GMD, to include neutral content-blocking devices that can protect high-voltage transmission lines;
- Discussion of the restoration and recovery capabilities of critical infrastructure under differing levels of damage and disruption; and
- Analysis of the feasibility of a real-time alert system to inform the electrical grid.

Some of these elements are addressed in *Appendix A: Technical Background*; and the Strategy's *Threat and Consequences Assessment*. The DHS Strategy will remain in effect for calendar years 2018–2026 and will be updated every two years.

Background

Extreme EMP and GMD incidents certainly fit into the categorization of "hard problems"—both are low probability/high consequence scenarios that challenge effective policymaking. A major electromagnetic incident caused by either EMP or GMD would pose immediate and simultaneous challenges to national and local decision-makers, Sector-Specific Agencies, private sector critical infrastructure owner-operators, and emergency managers at all levels of government. For example, significant uncertainties exist regarding the likely effects of extreme EMP and GMD events on existing civilian critical infrastructure. HEMP attacks by an adversary with basic nuclear weapons and missile capabilities may be disruptive on a regional scale, but are unlikely to cause catastrophic damage to the U.S. electric grid on a continental scale. Adversaries with highly developed nuclear capabilities might cause widespread harm to U.S. infrastructure with complex HEMP attacks in the context of an escalating international conflict. Space weather phenomena are relatively well understood within the scientific community, but the historical rarity of extreme GMD events limits availability of data useful for predictive analysis. Past events, such as the 1989 solar storm that led to the interruption of power in much of Québec for nearly nine hours, offer proof of the disruptive potential of GMD, as well as their potential to cascade impacts across critical infrastructure sectors and geographic regions.

The impacts to critical infrastructure resulting from electromagnetic incidents differ significantly from other large-scale, naturally occurring hazards, such as hurricanes. Many of the most harmful effects caused by electromagnetic incidents occur within milliseconds or seconds. These effects may simultaneously damage critical energy distribution nodes and industrial control systems over wide geographic areas through damage to microprocessors and power transformers. Such simultaneous disruptions over large areas of the country would likely undermine the implementation of mutual aid plans and agreements, a cornerstone of our approach to disaster response. Response and recovery may be further complicated by the relative lack of awareness of

electromagnetic threats and hazards in government and industry, the potential unavailability of communication systems, and the dearth of operational experience in dealing with the aftermath of electromagnetic incidents.

Therefore, it is imperative that the Department work with key stakeholders at all levels of government, and with relevant industries, to implement the goals of this Strategy.

While developing the DHS Strategy with key partners, several core principles were established that guide the themes and tenets of the Strategy:

- In the event of an electromagnetic incident, minimizing the loss of life and protecting and restoring critical infrastructure to pre-event levels should be the Department's highest priority.
- Assessments of electromagnetic incident risk in the planning stage of preparedness must be based upon sound science and, in the case of EMP, consensus Intelligence Community (IC) findings.
- Critical infrastructure protection activities should be prioritized based on risk management principles.
- The interdependence of critical infrastructure sectors must be accounted for when assessing risk and considering protective measures.
- Government and the private sector should share responsibility for critical infrastructure protection.
- Sharing of threat assessments and analyses among departments, critical infrastructure owners and operators, and private sector partners is critical to achieving a whole-of-Nation approach to preparing for, and responding to, electromagnetic incidents.

Strategy Summary

The DHS Strategy articulates three main EMP/GMD risk mitigation goals with key objectives identified under each goal.[9]

GOAL 1: Improve risk awareness of electromagnetic threats and hazards.[10]

DHS and critical stakeholders use technically informed risk assessments to support the electromagnetic-hazard research agenda, preparedness planning initiatives, and leadership decision-making.

Goal 1 Objectives

1.1 Improve EMP-related intelligence gathering, technical analysis, and information sharing to improve DHS and critical infrastructure stakeholder understanding of the EMP threat.

[9] Additional details, including sub-objectives are detailed in the body of the Strategy.

[10] "Electromagnetic threats and hazards" includes both EMP and GMD.

1.2 Increase coordination of intra-Departmental, Federal interagency, and civilian scientific research on EMP and GMD and their effects on critical infrastructure.

1.3 Provide timely distribution of information on credible electromagnetic threats and promote greater EMP and GMD awareness.

GOAL 2: Enhance capabilities to protect critical infrastructure from the impact of an electromagnetic incident.

DHS supports federal and industry partners to assure resilience of critical infrastructure and continuity of lifeline services and economically essential trade and commerce activities.

Goal 2 Objectives

2.1 Identify the national critical functions and associated infrastructure that need to be protected against an extreme electromagnetic incident, assess the systemic risk to these functions and infrastructure from such incidents, and determine whether existing plans meet the requirements for an effective recovery.

2.2 Increase the rigor and volume of analytical efforts to support advanced capabilities development for EMP-GMD protection, response, and recovery measures.

2.3 Identify and promote technological advances likely to significantly enhance resilience or reduce vulnerability of critical infrastructure to electromagnetic incidents.

GOAL 3: Promote effective electromagnetic-incident response and recovery efforts.

DHS supports national response and recovery efforts following an electromagnetic incident, including government continuity operations and mission-essential functions.

Goal 3 Objectives

3.1 Establish and maintain the capability to compile, analyze, and share electromagnetic incident information to enable appropriate response and recovery operations across all levels of government and with other non-governmental, private sector, and international entities, as appropriate.

3.2 Establish and maintain effective public risk communication plans to promote consistent messaging and address public uncertainty.

3.3 Develop, maintain, and exercise preparedness plans to enable effective and efficient recovery operations across Federal, state, local, tribal, and territorial (FSLTT) governments, critical owners and operators, and, as appropriate, with international, non-governmental, and private sector partners.

3.4 Provide recovery support and conduct long-term mitigation actions to promote resilience.

3.5 Ensure DHS is able to preserve the continuity of operations of primary mission-essential functions following an electromagnetic incident.

Implementation

DHS will use the DHS Strategy and corresponding Implementation Plan to identify, assign, execute, and track prioritized actions that will drive our comprehensive and coordinated national EMP-GMD protection efforts. This Strategy will also inform Departmental resource allocation

decisions, beginning with associated budget processes for FY 2020. Relevant DHS Office and Component heads will receive annual progress reports from the DHS Office of Strategy, Policy, and Plans regarding the implementation of the DHS Strategy. In FY 2018/2019, DHS will develop the companion Implementation Plan, including outlining lead and support roles, responsibilities, programs, and timelines for meeting the DHS Strategy's goals and objectives. DHS will utilize this Strategy and the Implementation Plan to support capability gap analyses and requirements generation.

Additionally, a draft executive order on coordinating national resilience to electromagnetic pulse incidents is currently being developed under the auspices of the National Security Council staff in coordination with Federal departments and agencies. Upon issuance, the executive order will obviously inform—and potentially alter—the Department's approach to the EMP-GMD threat that is articulated in this DHS Strategy.

Through the partnership structure described in the National Infrastructure Protection Plan, DHS will engage with public and private sector critical infrastructure partners to implement this Strategy.[11,12] DHS engagement with the private sector is critical to the Strategy's success, given that the majority of critical infrastructure potentially vulnerable to electromagnetic threats and hazards is privately owned. DHS does not have direct regulatory authority over these critical infrastructure sectors, and so realization of the goals, objectives, and end-states described in this strategy will not be possible without close and continued collaboration with the private sector and FSLTT partners.

Acknowledgments

This Strategy was developed by the DHS Office of Strategy, Policy, and Plans/Strategy, Planning, Analysis, and Risk (SPAR) in close coordination with the following DHS Offices and Components:

- Countering Weapons of Mass Destruction Office (CWMD);
- Federal Emergency Management Agency (FEMA);
- National Protection and Programs Directorate (NPPD);
- Office of the General Counsel (OGC);
- Office of Intelligence and Analysis (I&A);
- Office of Legislative Affairs (OLA);
- Science and Technology Directorate (S&T);
- United States Coast Guard (USCG); and
- Transportation Security Administration (TSA)

SPAR led a working group composed of members from each of these Offices and Components. In fulfilment of this Congressional requirement, DHS examined critical infrastructure vulnerabilities to electromagnetic incidents, considered updated Intelligence Community threat

[11] The SCCs are self-organized and self-governed councils that enable critical infrastructure owners and operators, their trade associations, and other industry representatives to interact on a wide range of sector-specific strategies, policies, and activities (see https://www.dhs.gov/scc).

[12] Upon Strategy approval, DHS will consult with the relevant Federal Sector-Specific Agencies and Sector Coordinating Councils for critical infrastructure to specifically identify and validate capability gaps and mechanisms to address them, including necessary resources and timelines.

assessments, reviewed scientific literature and ongoing research on electromagnetic phenomena, conducted engagements with interagency partners, and reviewed relevant Department and interagency policies and programs to inform this Strategy. SPAR also consulted with the Department of Energy's Office of Electricity Delivery and Energy Reliability and the Department of Defense's (DoD) Defense Threat Reduction Agency (DTRA) to ensure appropriate linkages exist between DHS initiatives and those of key interagency partners. SPAR engaged informally with industry stakeholders at informational meetings organized by DTRA and DOE, and at an annual Electric Infrastructure Security (EIS) Summit. DHS also consulted with members of the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack (EMP Commission) and carefully reviewed the Commission's research reports and threat assessments, which helped inform this Strategy.

Finally, through NPPD, DHS consulted with the critical infrastructure Sector-Specific Agencies (SSA) and the Sector Coordinating Councils (SCC).[13,14] The SCCs, in particular, provided insights related to local and regional issues relevant to critical infrastructure protection from potential electromagnetic threats and hazards.

[13] Federal SSAs include: DHS, DOE, DOD, Department of Treasury, U.S. Department of Agriculture, Department of Health and Human Services, General Services Administration, Department of Transportation, and Environmental Protection Agency. See https://www.dhs.gov/sector-specific-agencies for specific delineation of the SSA roles and responsibilities.

[14] Sector Coordinating Councils are self-organized and self-governed councils that enable private sector critical infrastructure owners and operators, their trade associations, and other industry representatives to interact on a wide range of sector-specific strategies, policies, and activities (https://www.dhs.gov/scc).

GOAL 1

Improve Risk Awareness of Electromagnetic Threats and Hazards

Current EMP-related intelligence gathering, sharing, and analysis remains largely stove-piped within the Federal Government and across DHS, which leads to disparate understanding of potential electromagnetic threats and hazards.[15] This problem also creates uncertainties about how DHS should address critical infrastructure vulnerabilities. In addition, government entities are often challenged in their ability to understand vulnerabilities and consequences to private and public sector critical infrastructure from EMP threats. These knowledge gaps make risk-informed decision-making difficult.

Assessments of the risks to civilian critical infrastructure from electromagnetic incidents are intrinsically difficult to produce due to the rarity—or complete absence—of actual events, as well as the fundamental complexity of predicting real-world interactions between electromagnetic pulses and thousands of diverse infrastructure installations.[16,17] As such, DHS and its private sector partners that own and operate critical infrastructure have significant uncertainty regarding risks posed by major electromagnetic events and, correspondingly, which (if any) mitigation techniques would address current vulnerabilities or increase resilience. These uncertainties make it difficult for DHS leadership and key private sector stakeholders to evaluate the return on investments made in preparedness actions and protection measures. In addition, information asymmetries among DHS and stakeholders increase these uncertainties and complicate efforts at coordinated action to mitigate electromagnetic incident risk among organizations with differing priorities and equities.

Finally, limited scientific research exists regarding the vulnerabilities of the electric grid and other critical infrastructure from the impacts of electromagnetic threats and hazards. Governmental, academic, and private sector entities need a more unified research effort to better inform risk assessments that support preparedness measures for the civilian sector. In addition, the Intelligence Community must leverage increases in scientific knowledge to continually refine intelligence collection protocols on the capabilities and intent of potential adversaries who may

---

[15] Threat, as defined by the *2010 DHS Risk Lexicon*, refers to an individual, entity, action, or occurrence; however, for the purpose of calculating risk, the threat of an intentional hazard is generally estimated as the likelihood of an attack (that accounts for both the intent and capability of the adversary) being attempted by an adversary; for other hazards, threat is generally estimated as the likelihood that a hazard will manifest.

[16] Risk can be estimated as a function of threat, vulnerability, and consequences. Risk is defined in the *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* "as the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.(See: https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf)

[17] Risk Assessment, as defined in the *2010 DHS Risk Lexicon*, is the product or process which collects information and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision-making.

attempt an EMP attack on the United States. Likewise, certain intelligence products may inform the scientific research agenda to improve EMP risk assessments.

To address these issues, DHS will take steps aligned with the objectives and sub-objectives below to improve intelligence-related capabilities, threat awareness and communication, and risk assessment capabilities. These steps will inform and enhance operational and resource decision-making within the Department and among critical infrastructure stakeholders.

Objective 1.1: Improve EMP-related intelligence gathering, technical analysis, and information sharing to enhance understanding of the EMP threat.

Sub-Objectives:

1.1.1 Provide substantive input to the National Intelligence Priority Framework to ensure that collection on EMP threats remains an IC priority.

1.1.2 Maintain up-to-date baseline intelligence and collection requirements for EMP threats to ensure DHS has access to timely and relevant information relative to changes in the EMP threat environment.

1.1.3 Produce intelligence-based, IC-coordinated EMP threat assessments that accurately define adversaries' intent and capabilities.

1.1.4 Share EMP threat information, as appropriate, to critical infrastructure owners and operators to improve situational awareness and decision-making.

Outcome: DHS and key critical infrastructure owners and operators have improved understanding of the threat posed by an intentional EMP attack.

Objective 1.2: Increase coordination of intra-Departmental, Federal interagency, and civilian scientific research on EMP and GMD and their effects on critical infrastructure.[18]

Sub-Objectives:

1.2.1. Review test data on the effects of EMP on critical infrastructure systems that are representative of those currently deployed throughout the Nation, including examination of prior research and analysis conducted by the Federal Government, academia, international partners, and industry to ensure the contemporary EMP and GMD research agenda is focused on known electromagnetic hazard knowledge gaps and avoids unnecessary duplication of effort.

1.2.2. Prioritize new tests of specific infrastructure associated with national critical functions deemed at greatest risk as identified in Sub-Objective 2.1.1.

1.2.3. Promote a public research agenda to encourage the private sector and academia to address known deficiencies in scientific knowledge to support unclassified electromagnetic hazard risk assessments.

[18] Actions taken in alignment of Objective 1.2 will be aligned with the National Critical Infrastructure Security and Resilience Research and Development Plan (https://www.dhs.gov/publication/national-critical-infrastructure-security-and-resilience-research-and-development-plan).

Outcome: *Scientific knowledge of electromagnetic phenomena relevant to electromagnetic-incident risk is increased across the Department, Federal interagency, and critical infrastructure sectors.*

Objective 1.3: Provide timely redistribution of information on credible electromagnetic threats and promote greater EMP-GMD awareness.

Sub-Objectives:

1.3.1. Disseminate EMP and GMD risk assessment information and research findings with relevant owners and operators of critical infrastructure using existing information-sharing platforms.

1.3.2. Conduct scientifically valid surveys of critical infrastructure owners and operators in relevant sectors to ascertain industry knowledge of electromagnetic threats and hazards, risk perceptions, research priorities, and levels of current or planned investment in resilience or mitigation measures.

1.3.3. Conduct a baseline assessment of Departmental and Federal interagency capabilities to produce validated electromagnetic risk assessments and modeling for steady-state and crisis-action situations.

1.3.4. Engage with emergency managers at all levels of government to encourage the planning and conduct of EMP-GMD preparedness activities such as training and exercises.

Outcome: *DHS and critical infrastructure stakeholders use validated risk assessments, including the probability and consequences of diverse electromagnetic hazards on critical infrastructure assets, to support the electromagnetic-hazard research agenda, preparedness planning initiatives, and informed leadership decision-making.*

GOAL 2

Enhance Capabilities to Protect Critical Infrastructure from the Impact of an Electromagnetic Incident

The protection calculus for critical infrastructure vulnerable to extreme EMP and GMD incidents is challenging, from detection and notification, to hardening, redundancy, and restoration. For example, translating scientific discovery into updated and more effective protective measures against electromagnetic threats is difficult due to the distributed ownership of the Nation's critical infrastructure and its diverse regulatory regime. Similarly, Federal Government networks operate under a distributed oversight model, making uniform protection standards difficult.

National means of detecting imminent GMD-hazard events and notifying critical infrastructure owners and operators exist, but analogous capabilities to address EMP threats require further development. In addition, potential disruption to the continuity of government (COG) by an electromagnetic event has not been fully assessed and remedied. This includes assessing what redundant capabilities may be needed to ensure the impact of electromagnetic incident is limited and infrastructure remains resilient.

These uncertainties in the probability and potential consequences of an electromagnetic incident make it difficult for key FSLTT and private sector critical infrastructure stakeholders to evaluate the return on investments made in potential protection measures. Information asymmetries among stakeholders increase these uncertainties and complicate efforts for coordinated action to mitigate risk. Commercial interests and the specter of regulatory enforcement create disincentives for owners and operators to openly share information about potential disruptions to their systems caused by electromagnetic events. DHS critical infrastructure protection efforts are largely centered on voluntary partnerships and heavily depend on information sharing. The Department actively supports vulnerability mitigation but does not generally have authority to compel it.

Objective 2.1: Identify the national critical functions and associated infrastructure that need to be protected against an extreme electromagnetic incident, assess the systemic risk to these functions and infrastructure from such incidents, and determine whether existing plans meet the requirements for an effective recovery.

Sub-Objectives:

2.1.1 In coordination with the SSAs and SCCs, identify the priority critical infrastructure, including space-based assets, that are acutely vulnerable to extreme

electromagnetic incidents and that, if disrupted, could reasonably result in catastrophic regional or national effects on national security, economic security, or public health or safety.

2.1.2 In coordination with the SSAs and SCCs, review existing restoration plans and capabilities for the critical infrastructure identified in Sub-Objective 2.1.1 and, as appropriate, identify consensus risk tolerances for such infrastructure within each sector.

2.1.3 Identify DHS-owned and operated mission-critical facilities' vulnerability to extreme electromagnetic incidents, prioritizing "lifeline" capabilities, and referencing existing governmental and non-governmental continuity, redundancy, and restoration standards and guidelines.[19]

Outcome: DHS has an improved, comprehensive awareness of those national critical functions and associated critical infrastructure systems, facilities, and networks that compel protection from an electromagnetic incident and where risk can be safely tolerated.

Objective 2.2: Increase the rigor and volume of analytical efforts to support advanced capabilities development for EMP-GMD protection, response, and recovery measures.

Sub-Objectives:

2.2.1 Identify how an electromagnetic incident would specifically impact individual critical infrastructure systems, utilities, and communications to better support the development of protective capabilities.

2.2.2 Determine and prioritize operational needs for responding to, and recovering from, an electromagnetic incident and enhance existing Departmental EMP-GMD response and recovery capabilities, where necessary.

2.2.3 In partnership with SSAs and SCCs, support and promote research seeking cost-effective approaches to reducing vulnerabilities to critical infrastructure from extreme EMP-GMD events.

Outcome: DHS and critical infrastructure owners and operators have a prioritized list of EMP-GMD operational needs and cost-effective solution options to improve electromagnetic protective measures.

Objective 2.3: Identify and promote technological advances likely to significantly enhance resilience or reduce vulnerability of critical infrastructure to electromagnetic incidents.

Sub-Objectives:

2.3.1. Identify those technologies and engineering approaches currently available to improve the resiliency of critical infrastructure to electromagnetic hazards, including physical protection of electric grid infrastructure, communications networks, and alert systems.

2.3.2. Explore the feasibility of establishing a forum on critical equipment interchangeability, supply chain resiliency, and mobility of spares composed of

[19] Lifeline critical infrastructure sectors include Electricity, Water and Wastewater, Transportation, and Communications.

representatives from relevant Sector-Specific Agencies and Sector Coordinating Councils.

2.3.3. Examine the vulnerability of the Nation's position, navigation, and timing (PNT) infrastructure, including lighted aids to navigation, both floating and fixed, and identify available mitigation technologies and engineering approaches.

Outcome: Critical infrastructure owners and operators use available technologies and measures to mitigate electromagnetic-incident risks as appropriate, ensuring continuity of lifeline services and economically essential activities in trade and commerce.

GOAL 3

Promote Effective Electromagnetic-Incident Response and Recovery Efforts

Response to, and recovery from, an extreme electromagnetic incident would pose immediate and simultaneous challenges to decision makers, Sector-Specific Agencies, private sector critical infrastructure owner-operators, and emergency managers at all levels of government. Many harmful effects associated with electromagnetic incidents occur within seconds or milliseconds and simultaneously affect critical infrastructure systems over wide geographic areas in ways that are difficult to predict in advance. Response and recovery may be further complicated by the lack of operational experience in dealing with electromagnetic incidents, including in an environment where communications may be impaired or nonexistent. Therefore, initial response actions may be uncertain and require alternative approaches to communication and decision-making relative to other natural or intentional threats and hazards. Longer-term recovery will also be challenging and require extended support at all levels of government, with critical infrastructure owners and operators, and with the private sector. The suite of existing operational plans, procedures, and capabilities applicable to manage the effects of all hazards may be adapted and maintained to address the unique requirements from an EMP strike or a space weather event.

Per Homeland Security Presidential Directive 5 (HSPD-5), "Management of Domestic Incidents," the Secretary of Homeland Security is the principal federal official for domestic incident management, and per the *Homeland Security Act of 2002*, as amended, the Secretary is also responsible for coordinating Federal operations within the United States to prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies. Utilizing the *National Response Framework* (NRF), DHS is responsible for coordinating federal operations within the United States to prepare for, respond to, and recover from an electromagnetic incident stemming from an intentional attack or natural space weather incident. As part of DHS's approach, the Department must understand the potential complexities in responding to, and recovering from, an electromagnetic incident and work with partners at the FSLTT levels and within the private sector to promote the security and resilience of the Nation.

Objective 3.1: Establish and maintain the capability to compile, analyze, and share electromagnetic incident information to enable appropriate response and recovery operations across all levels of government and with non-governmental, private sector, and international entities, as appropriate.

Sub-Objectives:

3.1.1. Establish, maintain, and exercise processes for electromagnetic-incident alerting, intelligence and information collection, analysis, and exchange within DHS and across multi-sectoral stakeholders in a potentially compromised communication

environment.

3.1.2. Enable the rapid sharing of validated electromagnetic-incident modeling information with appropriate stakeholders to support multi-sectoral decision-making throughout the response and recovery periods.

3.1.3. In coordination with relevant SSAs and SCCs, identify consensus recommendations for immediate protective actions to be taken in the event of an extreme electromagnetic incident alert.

Outcome: DHS and multi-sectoral stakeholders are able to share intelligence and information to support operational decision-making following alert of an electromagnetic incident.

Objective 3.2: Establish and maintain effective public risk communication plans to promote consistent messaging and address public uncertainty.

Sub-Objectives:

3.2.1. Ensure clarity of roles and responsibilities for lead agencies responsible for messaging to FSLTT response officials and critical infrastructure owners and operators.

3.2.2. Ensure provision of timely, regular, coordinated, and consistent risk communication, including information on response and recovery procedures across a range of media, accounting for the access and functional needs of the whole community, including messaging in multiple formats and languages.

Outcome: Effective public information and warning on extreme electromagnetic incidents is provided effectively to necessary stakeholders through a variety of mechanisms.

Objective 3.3: Develop, maintain, and exercise preparedness plans to enable effective and efficient response operations across FSLTT governments, critical infrastructure owners and operators, and, as appropriate, with international, non-governmental, and private sector partners.

Sub-Objectives:

3.3.1. Improve policies, plans, and guidance to ensure appropriate and timely FSLTT response and recovery actions are initiated to manage the consequences of electromagnetic incidents.

3.3.2. Systematically review after-action reports from previous EMP-GMD exercises to identify and disseminate recurring resource, capability, and authorities issues.

3.3.3. Develop guidelines to help account and plan for the access and functional needs of at-risk individuals in planning for electromagnetic incidents.

3.3.4. Incorporate EMP and GMD-related core capabilities and scenarios as regular design elements within the National Exercise Program.

3.3.5. Support the private sector in addressing any loss of critical infrastructure capability and capacity as quickly as possible to limit cascading electromagnetic-incident effects.

3.3.6. Adapt and augment mechanisms by which the Federal Government can use assistance from non-federal and foreign sources with necessary resources during an electromagnetic incident response.

Outcome: DHS, FSLTT, and industry partners execute operational plans to support an effective and efficient response.

Objective 3.4: Provide recovery support and conduct long-term mitigation actions to promote resilience.

Sub-Objectives:

3.4.1. Establish and maintain capabilities to provide rapid assessment of impacted critical infrastructure systems and prioritize their restoration based on their level of importance according to the risk analysis documented in Goal 1.

3.4.2. Support provision of long-term supplement of critical infrastructure capability loss to affected populations, including emergency responders.

Outcome: DHS is able to support FSLTT and private sector long-term recovery operations following the initial response to an electromagnetic incident.

Objective 3.5: Ensure DHS is able to preserve the continuity of operations of primary mission-essential functions following an electromagnetic incident.

Sub-Objectives:

3.5.1. Ensure DHS is prepared to secure, protect, and restore, as needed, critical infrastructure assets necessary for national essential functions and Homeland Security mission-essential functions that have the potential to impact or be impacted by an electromagnetic incident.

3.5.2. In coordination with the Electricity Subsector Coordinating Council, review the feasibility of rapidly isolating one or more portions of the North American electrical grid.

3.5.3. Ensure Departmental capacity to protect DHS equipment, facilities, and services throughout the event, specifically to ensure continuity of operations.

3.5.4. Employ national alert and warning infrastructure and maintain its operational effectiveness against electromagnetic hazards.

3.5.5. Employ continuity of government and continuity of operations plans that include contingencies for electromagnetic incidents (including the mitigation of impacts on critical infrastructure located within and outside the United States) to ensure continuation of national essential functions.

Outcome: DHS continues operations and is able to perform primary mission-essential functions following an electromagnetic incident.

Appendix A: Technical Background

This Appendix provides a technical background description of electromagnetic pulse (EMP) and geomagnetic disturbances (GMD), information which can better inform the reader of their potential impacts on the Nation's critical infrastructure.

Electromagnetic Pulse (EMP)

The term EMP means an electromagnetic pulse caused by a nuclear device or nonnuclear device, including such a pulse caused by an act of terrorism.[1] A *nuclear* electromagnetic pulse (NEMP) is a burst of electromagnetic (gamma) radiation created by a nuclear explosion that produces rapidly changing electric and magnetic fields. Given the potential impacts on critical infrastructure that may occur when these fields couple with electrical and electronic systems over a large geographic range, NEMP are the primary EMP concern for the Nation's homeland security.

The strength and area coverage of NEMP physical effects depends on the warhead type and yield, as well as the altitude and latitude of the detonation. The altitude of detonation is particularly critical because the damage effect is small for bursts below about 20 km altitude. This is due to the Earth's atmosphere being too dense to allow the electrons to travel far enough to "turn" appreciably. A nuclear device detonated at altitudes between 30 and 400 kilometers (a high-altitude EMP, or "HEMP"), however, would generate an EMP with amplitudes in the tens of kilovolts per meter with a radius of effects from hundreds to thousands of kilometers.[2] These high-altitude detonations therefore represent the greatest potential for severe impacts to the nation's critical infrastructure.

A HEMP event includes three waveforms: E1, E2, and E3 (see Figure 1):

[1] See 6 USC 101.

[2] U.S. Department of Energy, "Electromagnetic Pulse Resilience Action Plan" (2017), available at [https://www.energy.gov/sites/prod/files/2017/01/f34/DOE%20EMP%20Resilience%20Action%20Plan%20January%202017.pdf]

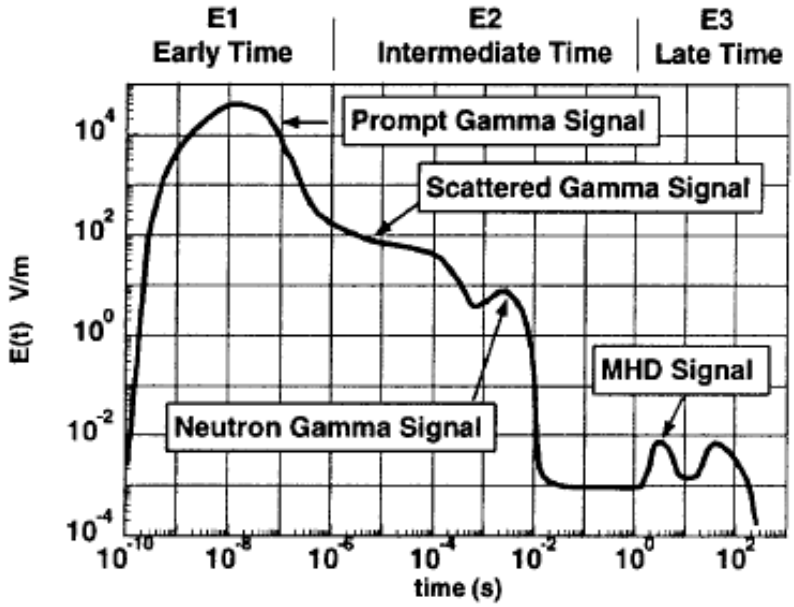


Figure 1: EMP Waveforms
Source: US Department of Energy, "Electromagnetic Pulse Resilience Action Plan," p.1.

The E1 waveform is a fast (i.e., nanosecond rise time, hundreds of nanoseconds duration), broad-band pulse that disrupts systems in general, including long-line electrical systems, computers, sensors, and electronic-based control systems. E1 can generate electric field strengths on the order of tens of thousands of volts per meter. E1 EMP can affect a wide area, but the intensity drops considerably from the area of maximum intensity, which is geomagnetically south of ground zero of a nuclear burst in the Northern Hemisphere.

The E2 waveform is longer and much lower in amplitude than the E1 waveform. As an intermediate time pulse, E2 manifests itself by enhancing the EMP currents on long lines in the microsecond and millisecond regime. The waveform is often described as being "like lightning" and while E2 current pulses are comparable to currents induced by nearby lightning strikes, the E2 pulse's magnitude is larger than lightning at higher frequencies; therefore the E2 and lightning protection standards are not equivalent.[3] In addition, because E2 follows E1, E2 protections may have failed due to the initial pulse.

Varying significantly from E1 and E2, the E3 waveform is a low-amplitude, long-duration pulse caused by a nuclear detonation at a high altitude which causes a temporary distortion of the Earth's magnetic field. E3 pulses are slow, lasting from tens to hundreds of seconds. E3 induces currents in so-called "long lines"—notably power and communication lines, pipelines, rail lines, and other vital elements of the Nation's critical infrastructure. These conductors act as antennas which may enhance magnetic field coupling and increase EMP/GMD effects, including destabilizing and damaging connected equipment such as electrical transformers.

[3] U.S. Army Corps of Engineers, *Engineering and Design: Electromagnetic Pulse (EMP) and Tempest Protection for Facilities* (1990). Available at [https://www.jrmagnetics.com/security/specs/EP_1110-3-2.pdf] (accessed May 7, 2018).

E3 waveform effects are comparable, but not equivalent, to those from geomagnetic disturbances. A GMD event typically features multiple peaks of pulses with varying amplitudes over hours or days; E3 typically is a singular pulse more intense and prolonged any one of these peaks.

EMP Exposure and Effects

EMP does not directly have any negative health or safety effects on humans and does not directly interfere with radio communications.[4] Electronics exposed to EMP, particularly semiconductor components, are at risk of upset; they may not function normally until cycled in power—or can be damaged through a surge in voltage or current.[5]

Significant uncertainty exists regarding EMP impacts both on an asset-level and system-level basis for infrastructure systems. For example, an E1 pulse may place any electronics within range at risk of upset or damage. However, existing shielding in some electronics, despite not being specifically designed to do so, may protect against EMP. Only some combination of shielding, grounding, and filtering, combined with verification testing, can ensure that electronics will function through an E1 EMP.[6] E3 has an effective wavelength larger than the Earth, so it does not couple with electronics and therefore does not directly affect electronics like E1 EMP. What it does is create a gradient in ground voltage. A very large conductor, such as the power grid that is grounded over distances of hundreds to thousands of kilometers and not properly configured, can experience a geomagnetically induced current (GIC) across the system because of voltage asymmetries. These asymmetries can, in turn, induce voltage collapse of the power grid from transformer saturation and damage to high-voltage transformer failure from internal heating.[7] Again, exact effects depend on many variables including local ground conductivity, details of transformer design, and the exact configuration of a power grid.

Geomagnetic Disturbance (GMD)

The term "GMD" refers to a geomagnetic disturbance caused by a solar storm or another naturally occurring phenomenon.[8] GMDs are caused by space weather events originating on the sun: naturally occurring sudden bursts of plasma and magnetic field structures (coronal mass ejections (CME) and bursts of radiation, or solar flares. These events tend to occur during the sun's "solar maximum," a four-to-six year period during the sun's regular cycle of reversing the polarities of its north and south poles.[9]

---

[4] "Electromagnetic Pulse," Risk Summary Sheet for the 2017 *Homeland Security National Risk Characterization* (HSNRC), a foundational analysis for DHS's 2018 *Quadrennial Homeland Security Review*. Other nuclear weapons effects and space weather effects can interfere with radio communications. See Samuel Glasstone and Phillip J. Dolan, eds., *The Effects of Nuclear Weapons*, 3rd ed. (Washington, D.C.: Department of Defense and Department of Energy, 1977).

[5] "Electromagnetic Pulse," Risk Summary Sheet.

[6] Lee, K.S.H., ed., *EMP Interaction: Principles, Techniques, and Reference Data* (Washington D.C.: Hemisphere Publishing Corporation, 1986).

[7] Wagner, V.E., et al., "Effects of Harmonics on Equipment," *IEEE Transactions on Power Delivery* 8, no. 2 (1993): 672-680.

[8] 6 USC 101.

[9] The sun's normal solar cycle runs 11 years. See North American Electric Reliability Corporation (NERC), "Introduction to GMD Studies," available at [http://www.nerc.com/pa/Stand/Project201303GeomagneticDisturbanceMitigation/GMD%20Planning%20Studies%20Workshop%20Presentation_120915.pdf] (accessed)

One to four days after an earth-directed flare or other eruption on the sun takes place, a GMD arrives at Earth and can cause multiple "space weather" effects.[10] This occurs when the CME interacts with the Earth's electrojet and causes changes in the magnetic field. As the GMD field couples to conductive surfaces on the ground, effects are similar to a slow-pulse E3, particularly on long-line network systems, such as the electrical power grid, communications lines, and pipelines. The extent of this effect varies based on the size of the system, the frequency and magnitude of the field, and environmental factors.

Of particular concern, GMD events can cause widespread blackouts by producing electromagnetic fields that induce extreme currents in wires, disrupting power lines and damaging large, high-voltage transformers. GMDs have the potential to impact large areas of the earth.[11] Unlike EMP, however, GMD events occur with regularity, raising the issue of not "if," but "when," the next event will occur, and what the impacts may be.

GMD Exposure and Effects

Like EMP, uncertainty exits regarding GMD events and their actual effects. These uncertainties result from a range of factors, including the infrequency of extreme events. Indeed, critical systems have not been tested by a major event in over 100 years. The destructive testing needed to reduce uncertainty about true vulnerability is costly to perform. Finally, it is unclear how rapidly the national economy and other aspects of the nation's operations would recover in circumstances in which power and communications infrastructure were significantly compromised.

The strongest geomagnetic storm on record is the Carrington Event of 1859 which electrified telegraph lines. The event caused major outages and disruptions in telegraph networks around the world; currents induced in the lines by the event were strong enough to cause sparks and allow some operators to disconnect their systems from batteries and send messages using only the current induced by the storm.[12] Impacts from the storm were limited given the state of technology at the time; modern society is far more vulnerable to the effects of a significant GMD event due to its reliance on electricity and technology. A more recent significant event occurred in 1989, when a geomagnetic storm collapsed the Hydro-Québec power grid in under two minutes, resulting in the loss of electric power to more than six million people for nine hours in Canada.

A Carrington-like event today, which exceeds the magnitude of the 1989 Hydro-Québec event, could even more significantly disrupt and damage electric power grids. A major GMD event could also disrupt radio communications and navigation signals from GPS satellites, and intense events could create significant radiation hazards for astronauts. Due to technological interdependencies, a severe GMD event could create a complex set of cascading effects, including requiring rerouting of air traffic to avoid areas where communication and navigation would be limited by space weather impacts.[13]

---

[10] Ibid.

[11] Ibid.

[12] National Research Council of the National Academies, "Severe Space Weather Events: Understanding Societal and Economic Impacts," (2008) accessible at [http://lasp.colorado.edu/home/wp-content/uploads/2011/07/lowres-Severe-Space-Weather-FINAL.pdf], accessed May 7, 2018.

[13] Ibid.

Summary

Table 1, below, offers a concise summary of EMP and GMD characteristics, including causes, warnings, effects, duration, and scope:

Table 1: EMP and GMD Characteristics

Attribute	EMP	GMD
Cause	Adversarial threat	Natural hazard
Warning	Strategic: unknown Tactical: none to several minutes	Strategic: 18 to 72 hours Tactical: 20 to 45 minutes
Effects	*E1:* High peak field – quick rise time *E2:* Medium peak field *E3:* low peak field, but quicker rise time and higher field than for GMD (possibly 3 times higher)	No comparable E1 wave forms No comparable E2 wave forms *E3:* low peak field – fluctuating magnitude and direction
Duration	*E1:* less than a 1 microsecond *E2:* less than 10 millisecond *E3 Blast:* ~10 seconds *E3 Heave:* ~1 – 2 minutes	No comparable E1 wave forms No comparable E2 wave forms *E3:* hours
Equipment at Risk	*E1:* telecommunications, electronics and control systems, relays, lightning arrestors *E2:* lightning: power lines and tower structures – "flashover", telecommunications, electronics, controls systems, transformers. *E3:* transformers and protective relays – long run transmission and communication - generator step-up transformers	*E3:* transformers and protective relays – long-haul transmission and communications – generator step-up transformers
Footprint	Regional to continental depending on height of burst	Regional to worldwide, depending upon magnitude
Geographic Variability	Can maximize coverage for E1 or E3 *E3:* intensity increases at the lower latitudes and as distance from ground zero is decreased or as yield is increased	*E3:* intensity increases near large bodies of water and generally at higher latitudes although events have been seen in southern latitudes

Source: U.S. Department of Energy, "Electromagnetic Pulse Resilience Action Plan," p.4