

# Electromagnetic Pulse (EMP)

## Program Status Report

August 17, 2020

Homeland Security

# EMP Program Status Report

## Table of Contents


Table of Contents ..... ii
I. Background ..... 1
II. Defining What is Critical ..... 2
III. DHS Preparedness Activities ..... 2
IV. Partnering with the Private Sector and Other Federal Departments ..... 3
V. Piloting EMP Risk Mitigation ..... 4
VI. Conclusion ..... 4

# I. Background

On March 26, 2019, President Trump signed Executive Order (E.O.) 13865, *Coordinating National Resilience to Electromagnetic Pulses*, which establishes resilience and security standards for U.S. critical infrastructure as a national priority initiative.[1]

E.O. 13865 states, "An electromagnetic pulse (EMP) has the potential to disrupt, degrade, and damage technology and critical infrastructure systems. Human-made or naturally occurring EMPs can affect large geographic areas, disrupting elements critical to the Nation's security and economic prosperity, and could adversely affect global commerce and stability. The federal government must foster sustainable, efficient, and cost-effective approaches to improving the Nation's resilience to the effects of EMPs."

Since the President signed E.O. 13865, the U.S. Department of Homeland Security (DHS) has worked to reduce risk from an EMP attack by seeking to develop a greater understanding of EMP effects on critical infrastructure, national critical functions, and national essential functions, and by taking key actions to address known EMP-related vulnerabilities to critical infrastructure. Our outreach and analysis are used to identify priorities for future security and mitigation efforts and to develop the case for private sector investment in technologies and capabilities that have a definable and traceable reduction of risk to the EMP threat. Based on this work, the Department will advise the public and private sectors on the most effective mitigation investments including, when appropriate, making recommendations to other federal departments and agencies.

The risk from EMP is a national issue with the potential to have a significant effect on critical infrastructure. Reducing the risk is a long-term effort. DHS is committed to this effort and is working to evaluate the need for a program management office to provide steady consistent leadership in both the public and private sector engagements.

In accordance with E.O. 13865, the Department has identified initial critical infrastructure and associated functions that are at greatest risk from an EMP and is focusing efforts on the development and implementation of evidence-based and independently-tested EMP protection and mitigation technologies and resilience best practices. Initial efforts within the Department, working across the federal interagency, have focused on risk management to both the Energy and Communications Sectors.

The E.O. required prioritization of systems, networks and assets related to the newly developed National Critical Functions (NCFs). The complexity of this task required the development of new models and concepts for prioritization. Development of these risk management concepts and models is ongoing. However, the models have matured to a point that enables prioritization of a limited set of systems, networks, and assets for EMP vulnerability assessments and mitigation efforts. While the development of these models took longer than initially envisioned, additional time was needed to validate the concepts and ensure the efficient application of resources to progress to subsequent tasks within the E.O.

[1] Executive Order on Coordinating National Resilience to Electromagnetic Pulses, March 26, 2019 www.whitehouse.gov/presidential-actions/executive-order-coordinating-national-resilience-electromagnetic-pulses/

## II. Defining What is Critical

DHS's Cybersecurity and Infrastructure Security Agency (CISA), through the National Risk Management Center (NRMC), leads the Department and interagency coordination and program management to plan and implement EMP executive and legislative requirements designated to DHS for implementation.

A month after the signing of the E.O., the NRMC, in coordination with Sector-Specific Agencies, established and released a preliminary set of NCFs.[2] The NCFs are government and private sector functions considered so vital to the U.S. that their disruption, corruption, or dysfunction would have debilitating effects on national security, economic security, public health or safety, or any combination thereof. The NCFs set the conditions for an analysis of system dependences specific to the EMP threat, as well as other scenarios of concern.

In addition to traditional models for determining criticality, DHS, in partnership with the federal interagency, is assessing how the widespread, simultaneous effects of an EMP would affect these criticality models. DHS is developing new concepts and approaches to evaluate how simultaneous common component failures could cause cascading failures across critical infrastructures, as well as hinder response and recovery operations due to a lack of repair parts and personnel. DHS is continuing to refine these models to support the development of the initial quadrennial EMP risk assessment and building vulnerability test plans in accordance with the E.O.

## III. DHS Preparedness Activities

In addition to defining what functions and infrastructure are critical, DHS, in coordination with the federal interagency, has developed initial planning guidance to assess operational plans to ensure that federal mission essential functions and services will continue during a disruptive event and in a post-EMP environment. As a leader in that effort, DHS is building EMP considerations into internal continuity and mission assurance plans and associated resourcing so that the Department is prepared to execute its Mission Essential Functions in the face of an EMP event.

In 2017, the Federal Emergency Management Agency (FEMA) and the Department of Energy (DOE) jointly developed the Power Outage Incident Annex: Managing the Cascading Impacts from a Long-Term Power Outage.[3] In 2020, FEMA, in consultation with the federal interagency, determined that the Power Outage Annex would serve as a baseline for emergency response planning associated with EMP. Based on that determination, DHS, along with other federal departments and agencies, have updated or are updating operational plans to align with the Annex's planning guidance.

---

[2] National Critical Functions Set, April 29, 2019 https://www.cisa.gov/national-critical-functions-set

[3] Power Outage Incident Annex to the Response and Recovery Federal Interagency Operational Plans, June 2017 https://www.fema.gov/media-library-data/1512398599047-7565406438d0820111177a9a2d4ee3c6/POIA_Final_7-2017v2_(Compliant_pda)_508.pdf

Related to this effort, FEMA manages the Emergency Alert System to notify the American public in the event of a national emergency, such as an impending EMP event. FEMA has designed and built EMP-hardened communications facilities to include Primary Entry Point stations which help to ensure the ability for the president to communicate with the nation in an emergency, to include preparation for, and response to, EMP events.[4] FEMA will continue to enhance EMP hardening of key facilities, validating their effectiveness against emerging threats like EMP and radio frequency weapons attacks.

FEMA is developing an interagency EMP exercise to be conducted in fiscal year 2021. The exercise will address the unique, widespread, cross-sector effects of an EMP event and challenge planning assumptions used by federal planners when considering EMP actions.

Since 2016, CISA and its predecessor organizations have promulgated *Electromagnetic Pulse (EMP) Protection and Resilience Guidelines for Critical Infrastructure and Equipment* for government and industry for mitigating the effects of EMP attacks on critical equipment and facilities. The Department is actively updating the EMP guidelines and anticipates reissuing in fiscal year 2020.

## IV. Partnering with the Private Sector and Other Federal Departments

The Department's priority for EMP resilience of critical infrastructure is energy and communications infrastructure. DHS and DOE have partnered to ensure unity of effort and efficient use of federal resources. One example of the collaboration is a partnership between DHS, DOE, and the Nuclear Regulatory Commission to validate the continued operation of key safety features of nuclear power plants in a post-EMP environment. This effort started in March of 2020 and will be completed in late 2021.

The DHS Science and Technology Directorate (S&T) developed a technology scouting report, cataloguing a number of available EMP protection equipment and testing organizations. This report highlights the variety of commercial equipment available to protect against an EMP. The initial version of this report was completed in June 2020 and will be available to federal agencies and private sector partners through the Homeland Security Information Network (HSIN). Beginning in 2020, S&T will conduct international engagements to further enhance our understanding of mitigation concepts and options employed by our international partners.

As funding becomes available, S&T, in coordination with CISA, will conduct vulnerability testing of prioritized critical infrastructure components, as well as validation testing of potentially applicable mitigation options for those components in order to better inform critical infrastructure owners and operators on what actions they can take to protect their systems.

[4] Primary Entry Point (PEP) stations are privately owned commercial and non-commercial radio broadcast stations that cooperatively participate with FEMA to provide emergency alert and warning information to the public before, during, and after a national or local emergency.

In 2019, CISA initiated and now leads a monthly Resilient Power Working Group (RPWG) with over 80 members from the private sector and federal, state and local, tribal, and territorial governments. The RPWG is developing the Resilient Power Guidelines, which will be used to support EMP mitigation planning and pilots. CISA and its predecessor organizations have led the federal Continuity Communications Community EMP mitigation planning efforts for the past decade.

## V. Piloting EMP Risk Mitigation

Finally, DHS is partnering with other federal departments and agencies, state, local, tribal, and territorial entities and the private sector to field test a more resilient critical infrastructure. There are a number of field demonstration (or pilot) projects planned and underway by both DHS and DOE to assess EMP vulnerability and then deploy, evaluate, and validate EMP mitigation and protection technologies. One such pilot is the San Antonio Electromagnetic Defense Initiative, designed to show how an entire region can become resilient against an EMP. These pilots are multisector, multifunction efforts, seeking to ensure key capabilities continue to function in a post EMP environment and that by maintaining those key functions we can expedite a full recovery. Working with federal interagency partners, DHS will play a major role in ensuring communications systems remain operational and, by ensuring key systems which are protected against EMP, are also protected against other threats such as cyber-attacks.

## VI. Conclusion

Recognizing that EMP presents a strategic threat to the nation, DHS continues to plan and execute on the President's and Congress's intent of sustainable, efficient, and cost-effective approaches to EMP mitigation. DHS will ensure collaboration across all relevant parties, continue to identify where the EMP threat presents the greatest risk to critical infrastructure, and focus efforts to ensure public and private sector mitigation efforts are scientifically based and have traceable reductions in the risk related to EMP. DHS is committed to all its missions, including ensuring federal continuity and safeguarding the American people, our homeland, and our values. Threats to our safety and security, including those from an EMP, are constantly evolving, and require continuous risk assessments and adaptive strategies to effectively address them. In the last year, the Department has made great progress and this work will continue—with a particular focus on partnership with industry in hardening critical infrastructure—in the next year and beyond.