

(A) Each classified and unclassified research and development project, and all appropriate details for each such project, including the component of the Department responsible for each such project.

(B) Each task order for a Federally Funded Research and Development Center not associated with a research and development project.

(C) Each task order for a University-based center of excellence not associated with a research and development project.

(D) The indicators developed and tracked by the Under Secretary for Science and Technology with respect to transitioned projects pursuant to subsection (c).

(2) Exception for certain completed projects

Paragraph (1) shall not apply to a project completed or otherwise terminated before December 23, 2016.

(3) Updates

The list required under paragraph (1) shall be updated as frequently as possible, but not less frequently than once per quarter.

(4) Research and development defined

For purposes of the list required under paragraph (1), the Secretary shall provide a definition for the term “research and development”.

(b) Requirement to report to Congress on all projects

Not later than January 1, 2017, and annually thereafter, the Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a classified and unclassified report, as applicable, that lists each ongoing classified and unclassified project at the Department, including all appropriate details of each such project.

(c) Indicators of success of transitioned projects

(1) In general

For each project that has been transitioned to practice from research and development, the Under Secretary for Science and Technology shall develop and track indicators to demonstrate the uptake of the technology or project among customers or end-users.

(2) Requirement

To the fullest extent possible, the tracking of a project required under paragraph (1) shall continue for the three-year period beginning on the date on which such project was transitioned to practice from research and development.

(d) Definitions

In this section:

(1) All appropriate details

The term “all appropriate details” means, with respect to a research and development project—

(A) the name of such project, including both classified and unclassified names if applicable;

(B) the name of the component of the Department carrying out such project;

(C) an abstract or summary of such project;

(D) funding levels for such project;

(E) project duration or timeline;

(F) the name of each contractor, grantee, or cooperative agreement partner involved in such project;

(G) expected objectives and milestones for such project; and

(H) to the maximum extent practicable, relevant literature and patents that are associated with such project.

(2) Classified

The term “classified” means anything containing—

(A) classified national security information as defined in section 6.1 of Executive Order 13526 (50 U.S.C. 3161 note) or any successor order;

(B) Restricted Data or data that was formerly Restricted Data, as defined in section 2014(y) of title 42;

(C) material classified at the Sensitive Compartmented Information (SCI) level, as defined in section 3345 of title 50; or

(D) information relating to a special access program, as defined in section 6.1 of Executive Order 13526 (50 U.S.C. 3161 note) or any successor order.

(3) Controlled unclassified information

The term “controlled unclassified information” means information described as “Controlled Unclassified Information” under Executive Order 13556 (50 U.S.C. 3501 note)¹ or any successor order.

(4) Project

The term “project” means a research or development project, program, or activity administered by the Department, whether ongoing, completed, or otherwise terminated.

(e) Limitation

Nothing in this section overrides or otherwise affects the requirements specified in section 468 of this title.

(Pub. L. 107–296, title III, § 319, as added Pub. L. 114–328, div. A, title XIX, § 1906(a), Dec. 23, 2016, 130 Stat. 2676.)

Editorial Notes

REFERENCES IN TEXT

Executive Order 13556, referred to in subsec. (d)(3), is set out as a note under section 3501 of Title 44, Public Printing and Documents.

PRIOR PROVISIONS

A prior section 319 of Pub. L. 107–296 was renumbered section 320 and is classified to section 195f of this title.

§ 195f. EMP and GMD mitigation research and development and threat assessment, response, and recovery

(a) In general

In furtherance of domestic preparedness and response, the Secretary, acting through the Under Secretary for Science and Technology,

¹ See References in Text note below.

and in consultation with other relevant executive agencies, relevant State, local, and tribal governments, and relevant owners and operators of critical infrastructure, shall, to the extent practicable, conduct research and development to mitigate the consequences of threats of EMP and GMD.

(b) Scope

The scope of the research and development under subsection (a) shall include the following:

(1) An objective scientific analysis—

(A) evaluating the risks to critical infrastructure from a range of threats of EMP and GMD; and

(B) which shall—

(i) be conducted in conjunction with the Office of Intelligence and Analysis; and

(ii) include a review and comparison of the range of threats and hazards facing critical infrastructure of the electrical grid.

(2) Determination of the critical utilities and national security assets and infrastructure that are at risk from threats of EMP and GMD.

(3) An evaluation of emergency planning and response technologies that would address the findings and recommendations of experts, including those of the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack, which shall include a review of the feasibility of rapidly isolating one or more portions of the electrical grid from the main electrical grid.

(4) An analysis of technology options that are available to improve the resiliency of critical infrastructure to threats of EMP and GMD, including an analysis of neutral current blocking devices that may protect high-voltage transmission lines.

(5) The restoration and recovery capabilities of critical infrastructure under differing levels of damage and disruption from various threats of EMP and GMD, as informed by the objective scientific analysis conducted under paragraph (1).

(6) An analysis of the feasibility of a real-time alert system to inform electrical grid operators and other stakeholders within milliseconds of a high-altitude nuclear explosion.

(c) Exemption from disclosure

(1) Information shared with the Federal Government

Section 673 of this title, and any regulations issued pursuant to such section, shall apply to any information shared with the Federal Government under this section.

(2) Information shared by the Federal Government

Information shared by the Federal Government with a State, local, or tribal government under this section shall be exempt from disclosure under any provision of State, local, or tribal freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring the disclosure of information or records.

(d) Threat assessment, response, and recovery

(1) Roles and responsibilities

(A) Distribution of information

(i) In general

Beginning not later than June 19, 2020, the Secretary shall provide timely distribution of information on EMPs and GMDs to Federal, State, and local governments, owners and operators of critical infrastructure, and other persons determined appropriate by the Secretary.

(ii) Briefing

The Secretary shall brief the appropriate congressional committees on the effectiveness of the distribution of information under clause (i).

(B) Response and recovery

(i) In general

The Administrator of the Federal Emergency Management Agency shall—

(I) coordinate the response to and recovery from the effects of EMPs and GMDs on critical infrastructure, in coordination with the heads of appropriate Sector-Specific Agencies, and on matters related to the bulk power system, in consultation with the Secretary of Energy and the Federal Energy Regulatory Commission; and

(II) to the extent practicable, incorporate events that include EMPs and extreme GMDs as a factor in preparedness scenarios and exercises.

(ii) Implementation

The Administrator of the Federal Emergency Management Agency, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, and on matters related to the bulk power system, the Secretary of Energy and the Federal Energy Regulatory Commission, shall—

(I) not later than June 19, 2020, develop plans and procedures to coordinate the response to and recovery from EMP and GMD events; and

(II) not later than December 21, 2020, conduct a national exercise to test the preparedness and response of the Nation to the effect of an EMP or extreme GMD event.

(C) Research and development

(i) In general

The Secretary, in coordination with the heads of relevant Sector-Specific Agencies, shall—

(I) without duplication of existing or ongoing efforts, conduct research and development to better understand and more effectively model the effects of EMPs and GMDs on critical infrastructure (which shall not include any system or infrastructure of the Department of Defense or any system or infrastructure of the Department of Energy associated with nuclear weapons activities); and

(II) develop technologies to enhance the resilience of and better protect critical infrastructure.

(ii) Plan

Not later than March 26, 2020, and in coordination with the heads of relevant Sector-Specific Agencies, the Secretary shall submit to the appropriate congressional committees a research and development action plan to rapidly address modeling shortfall and technology development.

(D) Emergency information system

(i) In general

The Administrator of the Federal Emergency Management Agency, in coordination with relevant stakeholders, shall maintain a network of systems, such as the alerting capabilities of the integrated public alert and warning system authorized under section 321o of this title, that are capable of providing appropriate emergency information to the public before (if possible), during, and in the aftermath of an EMP or GMD.

(ii) Briefing

Not later than December 21, 2020, the Administrator of the Federal Emergency Management Agency, shall brief the appropriate congressional committees regarding the maintenance of systems, including the alerting capabilities of the integrated public alert and warning system authorized under section 321o of this title.

(E) Quadrennial risk assessments

(i) In general

The Secretary, in coordination with the Secretary of Defense, the Secretary of Energy, and the Secretary of Commerce, and informed by intelligence-based threat assessments, shall conduct a quadrennial EMP and GMD risk assessment.

(ii) Briefings

Not later than March 26, 2020, and every four years thereafter until 2032, the Secretary, the Secretary of Defense, the Secretary of Energy, and the Secretary of Commerce shall provide a briefing to the appropriate congressional committees regarding the quadrennial EMP and GMD risk assessment.

(iii) Enhancing resilience

The Secretary, in coordination with the Secretary of Defense, the Secretary of Energy, the Secretary of Commerce, and the heads of other relevant Sector-Specific Agencies, shall use the results of the quadrennial EMP and GMD risk assessments to better understand and to improve resilience to the effects of EMPs and GMDs across all critical infrastructure sectors, including coordinating the prioritization of critical infrastructure at greatest risk to the effects of EMPs and GMDs.

(2) Coordination

(A) Report on technological options

Not later than December 21, 2020, and every four years thereafter until 2032, the

Secretary, in coordination with the Secretary of Defense, the Secretary of Energy, the heads of other appropriate agencies, and, as appropriate, private-sector partners, shall submit to the appropriate congressional committees, a report that—

(i) assesses the technological options available to improve the resilience of critical infrastructure to the effects of EMPs and GMDs; and

(ii) identifies gaps in available technologies and opportunities for technological developments to inform research and development activities.

(B) Test data

(i) In general

Not later than December 20, 2020, the Secretary, in coordination with the heads of Sector-Specific Agencies, the Secretary of Defense, and the Secretary of Energy, shall—

(I) review test data regarding the effects of EMPs and GMDs on critical infrastructure systems, networks, and assets representative of those throughout the Nation; and

(II) identify any gaps in the test data.

(ii) Plan

Not later than 180 days after identifying gaps in test data under clause (i), the Secretary, in coordination with the heads of Sector-Specific Agencies and in consultation with the Secretary of Defense and the Secretary of Energy, shall use the sector partnership structure identified in the National Infrastructure Protection Plan to develop an integrated cross-sector plan to address the identified gaps.

(iii) Implementation

The heads of each agency identified in the plan developed under clause (ii) shall implement the plan in collaboration with the voluntary efforts of the private sector, as appropriate.

(3) Definitions

In this subsection:

(A) The term “appropriate congressional committees” means—

(i) the Committee on Homeland Security and Governmental Affairs, the Committee on Armed Services, the Committee on Energy and Natural Resources, and the Committee on Commerce, Science, and Transportation of the Senate; and

(ii) the Committee on Transportation and Infrastructure, the Committee on Homeland Security, the Committee on Armed Services, the Committee on Energy and Commerce, and the Committee on Science, Space and Technology of the House of Representatives.

(B) The terms “prepare” and “preparedness” mean the actions taken to plan, organize, equip, train, and exercise to build and sustain the capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from those threats that pose the greatest risk to the se-

curity of the homeland, including the prediction and notification of impending EMPs and GMDs.

(C) The term “Sector Risk Management Agency” has the meaning given that term in section 650 of this title.

(e) Rule of construction

Nothing in this section may be construed—¹

(1) to affect in any manner the authority of the executive branch to implement Executive Order 13865, dated March 26, 2019, and entitled “Coordinating National Resilience to Electromagnetic Pulses”, or any other authority existing on the day before December 20, 2019, of any other component of the Department or any other Federal department or agency, including the authority provided to the Sector Risk Management Agency specified in section 61003(c) of division F of the Fixing America’s Surface Transportation Act (6 U.S.C. 121 note), including the authority under section 824o of title 16, and including the authority of independent agencies to be independent; or

(2) as diminishing or transferring any authorities vested in the Administrator of the Federal Emergency Management Agency or in the Agency prior to December 20, 2019.

(Pub. L. 107–296, title III, § 320, formerly § 319, as added Pub. L. 114–328, div. A, title XIX, § 1913(a)(3), Dec. 23, 2016, 130 Stat. 2685; renumbered § 320 and amended Pub. L. 115–278, § 2(g)(3)(B), (C), Nov. 16, 2018, 132 Stat. 4178; Pub. L. 116–92, div. A, title XVII, § 1740(a)(1), Dec. 20, 2019, 133 Stat. 1821; Pub. L. 116–283, div. H, title XC, § 9002(c)(2)(A), Jan. 1, 2021, 134 Stat. 4772; Pub. L. 117–263, div. G, title LXXI, § 7143(b)(2)(A), Dec. 23, 2022, 136 Stat. 3659.)

Editorial Notes

REFERENCES IN TEXT

Executive Order 13865, referred to in subsec. (e)(1), is Ex. Ord. No. 13865, Mar. 26, 2019, 84 F.R. 12041, which is set out as a note under this section.

Section 61003(c) of division F of the Fixing America’s Surface Transportation Act, referred to in subsec. (e)(1), is section 61003(c) of Pub. L. 114–94, div. F, Dec. 4, 2015, 129 Stat. 1778, which is set out as a note under section 121 of this title.

AMENDMENTS

2022—Subsec. (d)(3)(C). Pub. L. 117–263 substituted “section 650 of this title” for “section 651 of this title”.

2021—Subsec. (d)(3)(C). Pub. L. 116–283, § 9002(c)(2)(A)(i), substituted “Sector Risk Management Agency” for “Sector-Specific Agency”.

Subsec. (e)(1). Pub. L. 116–283, § 9002(c)(2)(A)(ii), substituted “Sector Risk Management Agency” for “Sector-Specific Agency”.

2019—Pub. L. 116–92, § 1740(a)(1)(A), inserted “and threat assessment, response, and recovery” after “development” in section catchline.

Subsecs. (d), (e). Pub. L. 116–92, § 1740(a)(1)(B), added subsecs. (d) and (e).

2018—Subsec. (c)(1). Pub. L. 115–278, § 2(g)(3)(C), substituted “Section 673 of this title” for “Section 133 of this title”.

Statutory Notes and Related Subsidiaries

BENCHMARKS; DEFINITIONS

Pub. L. 116–92, div. A, title XVII, § 1740(d), (h), Dec. 20, 2019, 133 Stat. 1824, 1825, provided that:

“(d) BENCHMARKS.—Not later than March 26, 2020, and as appropriate thereafter, the Secretary of Energy, in consultation with the Secretary of Defense, the Secretary of Homeland Security, and, as appropriate, the private sector, may develop or update, as necessary, quantitative and voluntary benchmarks that sufficiently describe the physical characteristics of EMPs, including waveform and intensity, in a form that is useful to and can be shared with owners and operators of critical infrastructure. Nothing in this subsection shall affect the authority of the Electric Reliability Organization to develop and enforce, or the authority of the Federal Energy Regulatory Commission to approve, reliability standards.

“(h) DEFINITIONS.—In this section [amending this section and section 347 of this title and enacting this note and provisions not set out in the Code]:

“(1) The term ‘appropriate congressional committees’ has the meaning given that term in subsection (d) of section 320 of the Homeland Security Act of 2002 [6 U.S.C. 195f(d)], as added by subsection (a) of this section; and

“(2) The terms ‘critical infrastructure’, ‘EMP’, and ‘GMD’ have the meanings given such terms in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101).”

Executive Documents

EX. ORD. NO. 13865. COORDINATING NATIONAL RESILIENCE TO ELECTROMAGNETIC PULSES

Ex. Ord. No. 13865, Mar. 26, 2019, 84 F.R. 12041, provided:

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

SECTION 1. *Purpose.* 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.

SEC. 2. *Definitions.* As used in this order:

(a) “Critical infrastructure” means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

(b) “Electromagnetic pulse” is a burst of electromagnetic energy. EMPs have the potential to negatively affect technology systems on Earth and in space. A high-altitude EMP (HEMP) is a type of human-made EMP that occurs when a nuclear device is detonated at approximately 40 kilometers or more above the surface of Earth. A geomagnetic disturbance (GMD) is a type of natural EMP driven by a temporary disturbance of Earth’s magnetic field resulting from interactions with solar eruptions. Both HEMPs and GMDs can affect large geographic areas.

(c) “National Critical Functions” means the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

(d) “National Essential Functions” means the overarching responsibilities of the Federal Government to lead and sustain the Nation before, during, and in the aftermath of a catastrophic emergency, such as an EMP that adversely affects the performance of Government.

(e) “Prepare” and “preparedness” mean the actions taken to plan, organize, equip, train, and exercise to build and sustain the capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and

¹ So in original. Probably should be “construed—”.

recover from those threats that pose the greatest risk to the security of the Nation. These terms include the prediction and notification of impending EMPs.

(f) A “Sector-Specific Agency” (SSA) is the Federal department or agency that is responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment. The SSAs are those identified in Presidential Policy Directive 21 of February 12, 2013 (Critical Infrastructure Security and Resilience).

SEC. 3. Policy. (a) It is the policy of the United States to prepare for the effects of EMPs through targeted approaches that coordinate whole-of-government activities and encourage private-sector engagement. The Federal Government must provide warning of an impending EMP; protect against, respond to, and recover from the effects of an EMP through public and private engagement, planning, and investment; and prevent adversarial events through deterrence, defense, and nuclear nonproliferation efforts. To achieve these goals, the Federal Government shall engage in risk-informed planning, prioritize research and development (R&D) to address the needs of critical infrastructure stakeholders, and, for adversarial threats, consult Intelligence Community assessments.

(b) To implement the actions directed in this order, the Federal Government shall promote collaboration and facilitate information sharing, including the sharing of threat and vulnerability assessments, among executive departments and agencies (agencies), the owners and operators of critical infrastructure, and other relevant stakeholders, as appropriate. The Federal Government shall also provide incentives, as appropriate, to private-sector partners to encourage innovation that strengthens critical infrastructure against the effects of EMPs through the development and implementation of best practices, regulations, and appropriate guidance.

SEC. 4. Coordination. (a) The Assistant to the President for National Security Affairs (APNSA), through National Security Council staff and in consultation with the Director of the Office of Science and Technology Policy (OSTP), shall coordinate the development and implementation of executive branch actions to assess, prioritize, and manage the risks of EMPs. The APNSA shall, on an annual basis, submit a report to the President summarizing progress on the implementation of this order, identifying gaps in capability, and recommending how to address those gaps.

(b) To further the Federal R&D necessary to prepare the Nation for the effects of EMPs, the Director of OSTP shall coordinate efforts of agencies through the National Science and Technology Council (NSTC). The Director of OSTP, through the NSTC, shall annually review and assess the R&D needs of agencies conducting preparedness activities for EMPs, consistent with this order.

SEC. 5. Roles and Responsibilities. (a) The Secretary of State shall:

(i) lead the coordination of diplomatic efforts with United States allies and international partners regarding enhancing resilience to the effects of EMPs; and

(ii) in coordination with the Secretary of Defense and the heads of other relevant agencies, strengthen nuclear nonproliferation and deterrence efforts, which would reduce the likelihood of an EMP attack on the United States or its allies and partners by limiting the availability of nuclear devices.

(b) The Secretary of Defense shall:

(i) in cooperation with the heads of relevant agencies and with United States allies, international partners, and private-sector entities as appropriate, improve and develop the ability to rapidly characterize, attribute, and provide warning of EMPs, including effects on space systems of interest to the United States;

(ii) provide timely operational observations, analyses, forecasts, and other products for naturally occurring EMPs to support the mission of the Department of

Defense along with United States allies and international partners, including the provision of alerts and warnings for natural EMPs that may affect weapons systems, military operations, or the defense of the United States;

(iii) conduct R&D and testing to understand the effects of EMPs on Department of Defense systems and infrastructure, improve capabilities to model and simulate the environments and effects of EMPs, and develop technologies to protect Department of Defense systems and infrastructure from the effects of EMPs to ensure the successful execution of Department of Defense missions;

(iv) review and update existing EMP-related standards for Department of Defense systems and infrastructure, as appropriate;

(v) share technical expertise and data regarding EMPs and their potential effects with other agencies and with the private sector, as appropriate;

(vi) incorporate attacks that include EMPs as a factor in defense planning scenarios; and

(vii) defend the Nation from adversarial EMPs originating outside of the United States through defense and deterrence, consistent with the mission and national security policy of the Department of Defense.

(c) The Secretary of the Interior shall support the research, development, deployment, and operation of capabilities that enhance understanding of variations of Earth’s magnetic field associated with EMPs.

(d) The Secretary of Commerce shall:

(i) provide timely and accurate operational observations, analyses, forecasts, and other products for natural EMPs, exclusive of the responsibilities of the Secretary of Defense set forth in subsection (b)(ii) of this section; and

(ii) use the capabilities of the Department of Commerce, the private sector, academia, and nongovernmental organizations to continuously improve operational forecasting services and the development of standards for commercial EMP technology.

(e) The Secretary of Energy shall conduct early-stage R&D, develop pilot programs, and partner with other agencies and the private sector, as appropriate, to characterize sources of EMPs and their couplings to the electric power grid and its subcomponents, understand associated potential failure modes for the energy sector, and coordinate preparedness and mitigation measures with energy sector partners.

(f) The Secretary of Homeland Security shall:

(i) provide timely distribution of information on EMPs and credible associated threats to Federal, State, and local governments, critical infrastructure owners and operators, and other stakeholders;

(ii) in coordination with the heads of any relevant SSAs, use the results of risk assessments to better understand and enhance resilience to the effects of EMPs across all critical infrastructure sectors, including coordinating the identification of national critical functions and the prioritization of associated critical infrastructure at greatest risk to the effects of EMPs;

(iii) coordinate response to and recovery from the effects of EMPs on critical infrastructure, in coordination with the heads of appropriate SSAs;

(iv) incorporate events that include EMPs as a factor in preparedness scenarios and exercises;

(v) in coordination with the heads of relevant SSAs, conduct R&D to better understand and more effectively model the effects of EMPs on national critical functions and associated critical infrastructure—excluding Department of Defense systems and infrastructure—and develop technologies and guidelines to enhance these functions and better protect this infrastructure;

(vi) maintain survivable means to provide necessary emergency information to the public during and after EMPs; and

(vii) in coordination with the Secretaries of Defense and Energy, and informed by intelligence-based threat assessments, develop quadrennial risk assessments on EMPs, with the first risk assessment delivered within 1 year of the date of this order [Mar. 26, 2019].

(g) The Director of National Intelligence shall:

(i) coordinate the collection, analysis, and promulgation, as appropriate, of intelligence-based assessments on adversaries' capabilities to conduct an attack utilizing an EMP and the likelihood of such an attack; and

(ii) provide intelligence-based threat assessments to support the heads of relevant SSAs in the development of quadrennial risk assessments on EMPs.

(h) The heads of all SSAs, in coordination with the Secretary of Homeland Security, shall enhance and facilitate information sharing with private-sector counterparts, as appropriate, to enhance preparedness for the effects of EMPs, to identify and share vulnerabilities, and to work collaboratively to reduce vulnerabilities.

(i) The heads of all agencies that support National Essential Functions shall ensure that their all-hazards preparedness planning sufficiently addresses EMPs, including through mitigation, response, and recovery, as directed by national preparedness policy.

SEC. 6. *Implementation.* (a) Identifying national critical functions and associated priority critical infrastructure at greatest risk.

(i) Within 90 days of the date of this order, the Secretary of Homeland Security, in coordination with the heads of SSAs and other agencies as appropriate, shall identify and list the national critical functions and associated priority critical infrastructure systems, networks, and assets, including space-based assets that, if disrupted, could reasonably result in catastrophic national or regional effects on public health or safety, economic security, or national security. The Secretary of Homeland Security shall update this list as necessary.

(ii) Within 1 year of the identification described in subsection (a)(i) of this section, the Secretary of Homeland Security, in coordination with the heads of other agencies as appropriate, shall, using appropriate government and private-sector standards for EMPs, assess which identified critical infrastructure systems, networks, and assets are most vulnerable to the effects of EMPs. The Secretary of Homeland Security shall provide this list to the President, through the APNSA. The Secretary of Homeland Security shall update this list using the results produced pursuant to subsection (b) of this section, and as necessary thereafter.

(b) Improving understanding of the effects of EMPs.

(i) Within 180 days of the identification described in subsection (a)(ii) of this section, the Secretary of Homeland Security, in coordination with the heads of SSAs and in consultation with the Director of OSTP and the heads of other appropriate agencies, shall review test data—identifying any gaps in such data—regarding the effects of EMPs on critical infrastructure systems, networks, and assets representative of those throughout the Nation.

(ii) Within 180 days of identifying the gaps in existing test data, as directed by subsection (b)(i) of this section, the Secretary of Homeland Security, in coordination with the heads of SSAs and in consultation with the Director of OSTP and the heads of other appropriate agencies, shall use the sector partnership structure identified in the National Infrastructure Protection Plan to develop an integrated cross-sector plan to address the identified gaps. The heads of agencies identified in the plan shall implement the plan in collaboration with the private sector, as appropriate.

(iii) Within 1 year of the date of this order, and as appropriate thereafter, the Secretary of Energy, in consultation with the heads of other agencies and the private sector, as appropriate, shall review existing standards for EMPs and develop or update, as necessary, quantitative benchmarks that sufficiently describe the physical characteristics of EMPs, including waveform and intensity, in a form that is useful to and can be shared with owners and operators of critical infrastructure.

(iv) Within 4 years of the date of this order, the Secretary of the Interior shall complete a magnetotelluric survey of the contiguous United States to help critical

infrastructure owners and operators conduct EMP vulnerability assessments.

(c) Evaluating approaches to mitigate the effects of EMPs.

(i) Within 1 year of the date of this order, and every 2 years thereafter, the Secretary of Homeland Security, in coordination with the Secretaries of Defense and Energy, and in consultation with the Director of OSTP, the heads of other appropriate agencies, and private-sector partners as appropriate, shall submit to the President, through the APNSA, a report that analyzes the technology options available to improve the resilience of critical infrastructure to the effects of EMPs. The Secretaries of Defense, Energy, and Homeland Security shall also identify gaps in available technologies and opportunities for future technological developments to inform R&D activities.

(ii) Within 180 days of the completion of the activities directed by subsections (b)(iii) and (c)(i) of this section, the Secretary of Homeland Security, in coordination with the heads of other agencies and in consultation with the private sector as appropriate, shall develop and implement a pilot test to evaluate available engineering approaches for mitigating the effects of EMPs on the most vulnerable critical infrastructure systems, networks, and assets, as identified in subsection (a)(ii) of this section.

(iii) Within 1 year of the date of this order, the Secretary of Homeland Security, in coordination with the heads of relevant SSAs, and in consultation with appropriate regulatory and utility commissions and other stakeholders, shall identify regulatory and non-regulatory mechanisms, including cost recovery measures, that can enhance private-sector engagement to address the effects of EMPs.

(d) Strengthening critical infrastructure to withstand the effects of EMPs.

(i) Within 90 days of completing the actions directed in subsection (c)(ii) of this section, the Secretary of Homeland Security, in coordination with the Secretaries of Defense and Energy and in consultation with the heads of other appropriate agencies and with the private sector as appropriate, shall develop a plan to mitigate the effects of EMPs on the vulnerable priority critical infrastructure systems, networks, and assets identified under subsection (a)(ii) of this section. The plan shall align with and build on actions identified in reports required by Executive Order 13800 of May 11, 2017 (Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure) [6 U.S.C. 1500 note prec.]. The Secretary of Homeland Security shall implement those elements of the plan that are consistent with Department of Homeland Security authorities and resources, and report to the APNSA regarding any additional authorities and resources needed to complete its implementation. The Secretary of Homeland Security, in coordination with the Secretaries of Defense and Energy, shall update the plan as necessary based on results from the actions directed in subsections (b) and (c) of this section.

(ii) Within 180 days of the completion of the actions identified in subsection (c)(i) of this section, the Secretary of Defense, in consultation with the Secretaries of Homeland Security and Energy, shall conduct a pilot test to evaluate engineering approaches used to harden a strategic military installation, including infrastructure that is critical to supporting that installation, against the effects of EMPs.

(iii) Within 180 days of completing the pilot test described in subsection (d)(ii) of this section, the Secretary of Defense shall report to the President, through the APNSA, regarding the cost and effectiveness of the evaluated approaches.

(e) Improving response to EMPs.

(i) Within 180 days of the date of this order, the Secretary of Homeland Security, through the Administrator of the Federal Emergency Management Agency, in coordination with the heads of appropriate SSAs, shall review and update Federal response plans, programs, and procedures to account for the effects of EMPs.

(ii) Within 180 days of the completion of actions directed by subsection (e)(i) of this section, agencies that support National Essential Functions shall update operational plans documenting their procedures and responsibilities to prepare for, protect against, and mitigate the effects of EMPs.

(iii) Within 180 days of identifying vulnerable priority critical infrastructure systems, networks, and assets as directed by subsection (a)(ii) of this section, the Secretary of Homeland Security, in consultation with the Secretaries of Defense and Commerce, and the Chairman of the Federal Communications Commission, shall provide the Deputy Assistant to the President for Homeland Security and Counterterrorism and the Director of OSTP with an assessment of the effects of EMPs on critical communications infrastructure, and recommend changes to operational plans to enhance national response and recovery efforts after an EMP.

SEC. 7. General Provisions. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

DONALD J. TRUMP.

[Reference to a Sector Specific Agency (including any permutations or conjugations thereof) deemed to be a reference to the Sector Risk Management Agency of the relevant critical infrastructure sector and have the meaning given such term in section 650 of this title, see section 652a(c)(3) of this title, enacted Jan. 1, 2021.]

§ 195g. Countering Unmanned Aircraft Systems Coordinator

(a) Coordinator

(1) In general

The Secretary shall designate an individual in a Senior Executive Service position (as defined in section 3132 of title 5) of the Department within the Office of Strategy, Policy, and Plans as the Countering Unmanned Aircraft Systems Coordinator (in this section referred to as the “Coordinator”) and provide appropriate staff to carry out the responsibilities of the Coordinator.

(2) Responsibilities

The Coordinator shall—

(A) oversee and coordinate with relevant Department offices and components, including the Office of Civil Rights and Civil Liberties and the Privacy Office, on the development of guidance and regulations to counter threats associated with unmanned aircraft systems (in this section referred to as “UAS”) as described in section 124n of this title;

(B) promote research and development of counter UAS technologies in coordination within the Science and Technology Directorate;

(C) coordinate with the relevant components and offices of the Department, including the Office of Intelligence and Analysis, to ensure the sharing of information, guidance, and intelligence relating to countering

UAS threats, counter UAS threat assessments, and counter UAS technology, including the retention of UAS and counter UAS incidents within the Department;

(D) serve as the Department liaison, in coordination with relevant components and offices of the Department, to the Department of Defense, Federal, State, local, and Tribal law enforcement entities, and the private sector regarding the activities of the Department relating to countering UAS;

(E) maintain the information required under section 124n(g)(3) of this title; and

(F) carry out other related counter UAS authorities and activities under section 124n of this title, as directed by the Secretary.

(b) Coordination with applicable Federal laws

The Coordinator shall, in addition to other assigned duties, coordinate with relevant Department components and offices to ensure testing, evaluation, or deployment of a system used to identify, assess, or defeat a UAS is carried out in accordance with applicable Federal laws.

(c) Coordination with private sector

The Coordinator shall, among other assigned duties, working with the Office of Partnership and Engagement and other relevant Department offices and components, or other Federal agencies, as appropriate, serve as the principal Department official responsible for sharing to the private sector information regarding counter UAS technology, particularly information regarding instances in which counter UAS technology may impact lawful private sector services or systems.

(Pub. L. 107–296, title III, § 321, as added Pub. L. 116–260, div. U, title VII, § 701(b)(1), Dec. 27, 2020, 134 Stat. 2295.)

§ 195h. National Urban Security Technology Laboratory

(a) In general

The Secretary, acting through the Under Secretary for Science and Technology, shall designate the laboratory described in subsection (b) as an additional laboratory pursuant to the authority under section 188(c)(2) of this title. Such laboratory shall be used to test and evaluate emerging technologies and conduct research and development to assist emergency response providers in preparing for, and protecting against, threats of terrorism.

(b) Laboratory described

The laboratory described in this subsection is the laboratory—

(1) known, as of December 27, 2021, as the National Urban Security Technology Laboratory; and

(2) transferred to the Department pursuant to section 183(1)(E) of this title.

(c) Laboratory activities

The National Urban Security Technology Laboratory shall—

(1) conduct tests, evaluations, and assessments of current and emerging technologies, including, as appropriate, the cybersecurity of such technologies that can connect to the internet, for emergency response providers;