

Presidential Documents

Executive Order 14143 of January 16, 2025

Providing for the Appointment of Alumni of AmeriCorps to the Competitive Service

By the authority vested in me as President by the Constitution and the laws of the United States of America, including sections 3301 and 3302 of title 5, United States Code, and section 301 of title 3, United States Code, it is hereby ordered as follows:

Section 1. *Policy.* The Federal Government benefits from a workforce that can be recruited from the broadest and deepest pools of qualified candidates for merit-based positions. The issuance of an order granting Non-Competitive Eligibility to certain alumni of programs administered by the Corporation for National and Community Service (operating as AmeriCorps) would be in the best interest of the Federal Government. AmeriCorps alumni have demonstrated a sustained commitment to public service, have received extensive training and hands-on experience, and have developed leadership, communication, and technical skills that are aligned with the missions of many federal agencies and departments. It is in the interest of the Federal Government to retain the services of these highly skilled individuals, particularly given that the Federal Government aided them in the acquisition of their skills.

Accordingly, pursuant to my authority under 5 U.S.C. 3302(1), and in order to achieve a workforce that is drawn from all segments of society as provided in 5 U.S.C. 2301(b)(1), I find that conditions of good administration make necessary an exception to the competitive hiring rules for certain positions in the Federal civil service.

Sec. 2. *Establishment.* The head of any executive department or agency may appoint noncompetitively any individual who is certified under section 3 of this order to a position in the competitive service for which the individual is qualified.

Sec. 3. *Certifications.* (a) The Chief Executive Officer (CEO) of AmeriCorps, or the CEO's designee, shall issue certificates to persons whom the CEO or designee deems to have satisfactorily completed:

(i) a full-time term of national service of at least 1,700 hours as a Team Leader or Member, as specified in section 155(b)(1) or 155(b)(4) of the National and Community Service Act of 1990 (42 U.S.C. 12615(b)(1), 12615(b)(4)), or in the AmeriCorps National Civilian Community Corps program component specified in section 153 of that Act (42 U.S.C. 12613); or

(ii) one or more terms of service that total at least 1,700 hours under section 139(b)(1) of that Act (42 U.S.C. 12593(b)(1)) as an AmeriCorps State and National participant under section 137 of that Act (42 U.S.C. 12591).

(b) This order does not alter or otherwise affect the Non-Competitive Eligibility status for AmeriCorps Volunteers in Service to America participants, commonly known as VISTA members, who successfully complete their service, as described in section 415(d) of the Domestic Volunteer Service Act of 1973, as amended (42 U.S.C. 5055(d)).

(c) In making any certification under this section, the CEO, or the CEO's designee, may rely on a confirmation made by the entity that selected the individual for, and supervised the individual in, the approved national

service position in which such individual successfully completed a term of service, as specified in this section. If AmeriCorps determines that the certification is incorrect, the Corporation shall, after considering the full facts and circumstances surrounding the incorrect certification, take appropriate action.

(d) Any appointment under this order shall be effected within 1 year after completion of the appointee's most recent term of service in the programs described in subsections (a)(i)–(ii) of this section. Such period may be extended to not more than 3 years for persons who, following participation in the programs described in subsections (a)(i)–(ii) of this section, are engaged in an additional term of AmeriCorps service, in military service, in the pursuit of studies at an institution of higher learning, or in other activities that, in the view of the appointing authority, warrant an extension of such period. Such period may also be extended to permit the adjudication of a background investigation.

(e) Any law, Executive Order, or regulation that would disqualify an applicant for appointment in the competitive service shall also disqualify an applicant for appointment under this order. Examples of disqualifying criteria include restrictions on employing persons who are not United States citizens or nationals; who have violated 5 U.S.C. 2302(b)(7) and 3310 (the anti-nepotism provisions of the Civil Service Reform Act of 1978); who have knowingly and willfully failed to register for Selective Service when required to do so, 5 U.S.C. 3328(a)(2); who do not meet occupational qualifying standards prescribed by the Office of Personnel Management (OPM); or who do not meet suitability factors prescribed by OPM.

Sec. 4. Regulations. The Director of OPM is authorized to issue such additional regulations as may be necessary to implement this order. Any individual who meets the terms of this order, however, is eligible for noncompetitive hiring with or without additional regulations.

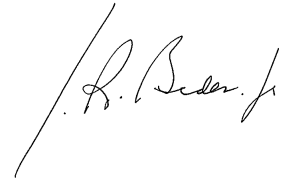
Sec. 5. General Provisions. (a) Nothing in this order shall be construed to impair or otherwise affect:

(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.



THE WHITE HOUSE,
January 16, 2025.

Presidential Documents

Executive Order 14139 of January 3, 2025

Providing an Order of Succession Within the Office of the National Cyber Director

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the Federal Vacancies Reform Act of 1998, as amended, 5 U.S.C. 3345 *et seq.* (the “Act”), it is hereby ordered that:

Section 1. *Order of Succession.* Subject to the provisions of section 2 of this order, and to the limitations set forth in the Act, the following officials of the Office of the National Cyber Director, in the order listed, shall act as and perform the functions and duties of the office of the National Cyber Director (Director) during any period in which the Director has died, resigned, or otherwise become unable to perform the functions and duties of the office of Director:

- (a) Deputy National Cyber Director;
- (b) Chief of Staff;
- (c) Assistant National Cyber Director for Policy Development;
- (d) Assistant National Cyber Director for Policy Implementation;
- (e) Assistant National Cyber Director for Resource Management and Administration; and
- (f) General Counsel.

Sec. 2. *Exceptions.* (a) No individual who is serving in an office listed in section 1(a)–(f) of this order in an acting capacity shall, by virtue of so serving, act as Director pursuant to this order.

(b) No individual who is serving in an office listed in section 1(a)–(f) of this order shall act as Director unless that individual is otherwise eligible to so serve under the Act.

(c) Notwithstanding the provisions of this order, the President retains discretion, to the extent permitted by law, to depart from this order in designating an acting Director.

Sec. 3. *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.

Presidential Documents

Title 3—**Executive Order 14142 of January 15, 2025****The President****Taking Additional Steps With Respect to the Situation in Syria**

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the International Emergency Economic Powers Act (50 U.S.C. 1701 *et seq.*), the National Emergencies Act (50 U.S.C. 1601 *et seq.*), section 212(f) of the Immigration and Nationality Act of 1952 (8 U.S.C. 1182(f)), and section 301 of title 3, United States Code,

I, JOSEPH R. BIDEN JR., President of the United States of America, in view of changing circumstances on the ground in Syria and in order to take additional steps with respect to the national emergency declared in Executive Order 13894 of October 14, 2019 (Blocking Property and Suspending Entry of Certain Persons Contributing to the Situation in Syria), hereby order:

Section 1. *Amendments to Executive Order 13894.* Executive Order 13894 is hereby amended by:

(a) striking from the second paragraph the phrase “, and in particular the recent actions by the Government of Turkey to conduct a military offensive into northeast Syria,”;

(b) striking subsections (1)(a)(i)(B)–(F) and inserting, in lieu thereof, the following:

“(B) to have materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, any person whose property and interests in property are blocked pursuant to this order; or

(C) to be owned or controlled by, or to have acted or purported to act for or on behalf of, directly or indirectly, any person whose property and interests in property are blocked pursuant to this order.”; and

(c) striking subsection 8(f).

Sec. 2. *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.

Presidential Documents

Title 3—

Executive Order 14141 of January 14, 2025

The President

Advancing United States Leadership in Artificial Intelligence Infrastructure

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. Artificial intelligence (AI) is a defining technology of our era. Recent advancements in AI demonstrate its rapidly growing relevance to national security, including with respect to logistics, military capabilities, intelligence analysis, and cybersecurity. Building AI in the United States will help prevent adversaries from gaining access to, and using, powerful future systems to the detriment of our military and national security. It will also enable the United States Government to continue harnessing AI in service of national-security missions while preventing the United States from becoming dependent on other countries' infrastructure to develop and operate powerful AI tools.

Advances at the frontier of AI will also have significant implications for United States economic competitiveness. These imperatives require building AI infrastructure in the United States on the time frame needed to ensure United States leadership over competitors who, already, are racing to take the lead in AI development and adoption. Building AI in the United States requires enormous private-sector investments in infrastructure, especially for the advanced computing clusters needed to train AI models and the energy infrastructure needed to power this work. Already, AI's electricity and computational needs are vast, and they are set to surge in the years ahead. This work also requires secure, reliable supply chains for critical components needed to build AI infrastructure, from construction materials to advanced electronics.

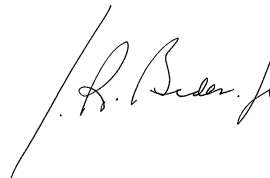
This order sets our Nation on the path to ensure that future frontier AI can, and will, continue to be built here in the United States. In building domestic AI infrastructure, our Nation will also advance its leadership in the clean energy technologies needed to power the future economy, including geothermal, solar, wind, and nuclear energy; foster a vibrant, competitive, and open technology ecosystem in the United States, in which small companies can compete alongside large ones; maintain low consumer electricity prices; and help ensure that the development of AI infrastructure benefits the workers building it and communities near it.

With this order, I provide a plan for protecting national security, preserving our economic competitiveness, revitalizing our energy infrastructure, and ensuring United States leadership in AI.

Sec. 2. Policy. It is the policy of the United States to enable the development and operation of AI infrastructure, including data centers, in the United States in accordance with five guiding principles. When undertaking the actions set forth in this order, executive departments and agencies (agencies) shall adhere to these principles, as appropriate and consistent with applicable law:

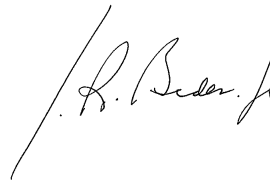
(a) The development of AI infrastructure should advance United States national security and leadership in AI. Meeting this goal will require steps by the Federal Government, in collaboration with the private sector, to advance AI development and use AI for future national-security missions, including through the work described in National Security Memorandum 25 of October 24, 2024 (Advancing the United States' Leadership in Artificial

(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 persons.



THE WHITE HOUSE,
January 15, 2025.

(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.



THE WHITE HOUSE,
January 3, 2025.

Intelligence; Harnessing Artificial Intelligence to Fulfill National Security Objectives; and Fostering the Safety, Security, and Trustworthiness of Artificial Intelligence) (NSM–25). It will also require the use of safeguards to improve the cyber, supply-chain, and physical security of the laboratories at which powerful AI is developed, stored, and used. Additionally, protecting United States national security will require further work to evaluate and manage risks related to the powerful capabilities that future frontier AI may possess.

(b) The development of AI infrastructure should advance United States economic competitiveness, including by fostering a vibrant technology ecosystem. Already, AI is creating new jobs and industries, and its effects are being felt in sectors across the economy. The Federal Government must ensure that the United States remains competitive in the global economy, including through harnessing the benefits of this technology for all Americans. It must also promote a fair, open, and competitive AI ecosystem so that small developers and entrepreneurs can continue to drive innovation—a priority highlighted in both Executive Order 14110 of October 30, 2023 (Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence), and NSM–25—as well as to support secure, reliable supply-chain infrastructure for AI activities.

(c) The United States can and should lead the world in operating the next generation of AI data centers with clean power. Meeting this goal will require building on recent successes to modernize our Nation’s energy infrastructure; improve permitting processes; and support investments in, and expeditious development of, both currently available and emerging clean energy technologies, such as geothermal energy, nuclear energy, and long-duration energy storage used to store clean energy, as well as relevant supply chains. The United States must not be surpassed in its support for the development, commercialization, and operation of clean energy technologies at home and abroad, and the rapid buildout of AI infrastructure offers another vital opportunity to accelerate and deploy these energy technologies. To help ensure that new data center electricity demand does not take clean power away from other end users, result in resource adequacy issues, or increase grid emissions, the construction of AI infrastructure must be matched with new, clean electricity generation resources.

(d) The development of AI infrastructure should proceed without raising energy costs for American consumers and businesses, and it should have strong community support. The companies developing, commercializing, and deploying AI must finance the cost of building the infrastructure needed for AI operations, including the development of next-generation power infrastructure built for these operations.

(e) The development of AI infrastructure should benefit those working to build it. Meeting this goal will require high labor standards and safeguards for the buildout of AI infrastructure, consultation and close collaboration with communities affected by this infrastructure’s development and operation, and continuous work to mitigate risks and potential harms. The American people more broadly must safely enjoy the gains and opportunities from technological innovation in the AI ecosystem.

Sec. 3. Definitions. For purposes of this order:

(a) The term “agency” means each agency described in 44 U.S.C. 3502(1), except for the independent regulatory agencies described in 44 U.S.C. 3502(5).

(b) The term “AI data center” means a data center used primarily with respect to developing or operating AI.

(c) The term “AI infrastructure” refers collectively to AI data centers, generation and storage resources procured to deliver electrical energy to data centers, and transmission facilities developed or upgraded for the same purpose.

(d) The term “AI model” means a component of an information system that implements AI technology and uses computational, statistical, or machine-learning techniques to produce outputs from a given set of inputs.

(e) The term “clean energy” or “clean energy generation resources” means generation resources that produce few or no emissions of carbon dioxide during operation, including when paired with clean storage technologies. This term includes geothermal, nuclear fission, nuclear fusion, solar, wind, hydroelectric, hydrokinetic (including tidal, wave, and current), and marine energy; and carbon capture, utilization, and storage technologies (for which the carbon capture equipment meets the definition set forth in 26 C.F.R. 1.45Q–2(c)) that operate with fossil fuel generation resources, that achieve carbon dioxide capture rates of 90 percent or higher on an annual basis, and that permanently sequester the captured carbon dioxide.

(f) The term “clean power” means electricity generated by the generation resources described in subsection (e) of this section.

(g) The term “clean repowering” means the practice of siting new clean generation sources at a site with an existing point of interconnection and generation sources operating with fossil fuels, such that some output or capacity from existing generation sources is replaced by the new clean generation sources.

(h) The term “critical electric infrastructure information” has the same meaning as set forth in 18 C.F.R. 388.113(c).

(i) The term “data center” means a facility used to store, manage, process, and disseminate electronic information for a computer network, and it includes any facility that is composed of one or more permanent or semi-permanent structures, or that is a dedicated space within such structure, and operates persistently in a fixed location; that is used for the housing of information technology equipment, including servers, mainframe computers, high-performance computing devices, or data-storage devices; and that is actively used for the hosting of information and information systems that are accessed by other systems or by users on other devices.

(j) The term “distributed energy resource” has the same meaning as set forth in 18 C.F.R. 35.28(b)(10).

(k) The term “Federal Permitting Agencies” refers to the agency members of the Federal Permitting Improvement Steering Council (Permitting Council) established under section 41002 of the Fixing America’s Surface Transportation (FAST) Act, 42 U.S.C. 4370m–1, as well as any other agency with authority to issue a Federal permit or approval required for the development or operation of AI infrastructure.

(l) The term “Federal Risk and Authorization Management Program” refers to the program established to provide an approach for the adoption and use of cloud services by the Federal Government, as codified in 44 U.S.C. 3607–3616 (as enacted by the FedRAMP Authorization Act, section 5921 of Public Law 117–263).

(m) The term “frontier AI data center” means an AI data center capable of being used to develop, within a reasonable time frame, an AI model with characteristics related either to performance or to the computational resources used in its development that approximately match or surpass the state of the art at the time of the AI model’s development.

(n) The term “frontier AI infrastructure” means AI infrastructure for which the relevant data center is a frontier AI data center.

(o) The term “frontier AI training” refers to the act of developing an AI model with characteristics related either to performance or to the computational resources used in its development that approximately match or surpass the state of the art at the time of the AI model’s development.

(p) The term “generation resource” means a facility that produces electricity.

or cultural resources; threatened or endangered species; and harbors or river improvements not associated with hydropower generation resources;

(iii) proximity to any communities seeking to host AI infrastructure, including for reasons related to local workers' access to jobs involved in designing, building, maintaining, and operating data centers;

(iv) ready access and proximity to high-voltage transmission infrastructure that minimizes the scale of, cost of, and timeline to develop any transmission upgrades or development needed to interconnect AI infrastructure, in consideration of access and proximity to:

(A) high-capacity transmission infrastructure with unused capacity, as identified by collection activities described in section 6 of this order;

(B) any planned generation facilities that can enable delivery of electricity to an AI data center on the site managed by each Secretary's respective agency, that possess an executed interconnection agreement with a transmission provider, that do not possess an executed power purchase agreement, and for which construction has not yet begun;

(C) any lands that the Secretary of the Interior identifies pursuant to subsection (c) of this section; and

(D) any power generation facilities with high clean repowering potential;

(v) location within geographic areas that are not at risk of persistently failing to attain National Ambient Air Quality Standards, and where the total cancer risk from air pollution is at or below the national average according to the Environmental Protection Agency's (EPA's) 2020 AirToxScreen;

(vi) lack of proximity to waters of the United States for purposes of permitting requirements;

(vii) lack of extensive restrictions on land uses associated with constructing and operating AI infrastructure or on access to necessary rights-of-way for such activities;

(viii) ready access to high-capacity telecommunications networks;

(ix) suitability for the development of access roads or other temporary infrastructure necessary for the construction of AI infrastructure; and

(x) absence of other characteristics that would, if the site was used or repurposed for AI infrastructure, compromise a competing national security concern as determined by the relevant Secretary in consultation with the Assistant to the President for National Security Affairs.

(b) By March 15, 2025, the Secretary of the Interior, acting through the Director of the Bureau of Land Management (BLM), in consultation with the Secretary of Defense, the Secretary of Energy, and the Chair of the Federal Energy Regulatory Commission, shall identify sites managed by BLM that the Secretary of the Interior, acting through the Director of BLM, deems may be suitable for granting or issuing rights of way to private-sector entities to construct and operate additional clean energy facilities that are being or may be built as components of frontier AI infrastructure developed pursuant to this section. In performing this work, the Secretary of the Interior, in consultation with the Secretary of Defense and the Secretary of Energy, shall take steps to ensure where feasible and appropriate that any such sites identified under this subsection include sufficient acreage for developing clean generation resources that can deliver sufficient electricity to each site identified under subsection (a) of this section for matching the capacity needs of frontier AI data centers on the latter sites. The sites identified under this subsection shall include any land managed by the Department of the Interior that is within a region designated by the Secretary of the Interior under subsection (c) of this section, or a region preliminarily identified as a candidate for such designation. In determining the suitability of sites, the Secretary of the Interior, acting through the Director of BLM, shall prioritize identification of sites that:

(q) The terms “interconnection,” “interconnection facilities,” and “point of interconnection” refer to facilities and equipment that physically and electrically connect generation resources or electrical load to the electric grid for the purpose of the delivery of electricity, for which grid operators have granted all appropriate approvals required for those facilities and equipment to operate.

(r) The term “lab-security measures” refers to steps to detect, prevent, or mitigate physical, cyber, or other threats to the operation of a data center, to the integrity of information or other assets stored within it, or of unauthorized access to such information or assets.

(s) The term “leading-edge logic semiconductors” refers to semiconductors produced at high volumes using extreme ultraviolet lithography tools as defined by the CHIPS Incentives Program Notice of Funding Opportunity, 2023–NIST–CHIPS–CFF–01.

(t) The term “model weight” means a numerical parameter within an AI model that helps determine the model’s outputs in response to inputs.

(u) The term “new source review” refers to the permitting program with this name in 40 C.F.R. parts 51 or 52.

(v) The term “non-Federal parties” refers to private-sector entities that enter into a contract with the Department of Defense or the Department of Energy pursuant to section 4(g) of this order.

(w) The term “priority geothermal zone” refers to lands with high potential for the development of geothermal power generation resources, as designated by the Secretary of the Interior, including pursuant to section 4(c) of this order.

(x) The term “project labor agreement” means a pre-hire collective bargaining agreement that establishes the terms and conditions of a construction project.

(y) The term “surplus interconnection service” has the same meaning as set forth in Federal Energy Regulatory Commission Order No. 845.

(z) The terms “transmission facilities” and “transmission infrastructure” mean equipment or structures, including transmission lines and related facilities, used for the purpose of delivering electricity.

(aa) The term “transmission organization” refers to a Regional Transmission Organization or an Independent System Operator.

(bb) The term “transmission provider” means an entity that manages or operates transmission facilities for the delivery of electric energy used primarily by the public and that is not a transmission organization.

(cc) The term “waters of the United States” has the same meaning as set forth in 33 C.F.R. 328.3(a).

Sec. 4. Establishing Federal Sites for AI Infrastructure. (a) By February 28, 2025, the Secretary of Defense and the Secretary of Energy shall, if possible, each identify a minimum of 3 sites on Federal land managed by their respective agencies that may be suitable for the agencies to lease to non-Federal entities for the construction and operation of a frontier AI data center, as well as for the construction and operation of clean energy facilities to serve the data center, by the end of 2027. In identifying these sites, each Secretary shall, as feasible and appropriate, seek to prioritize sites that possess the following characteristics, as consistent with the objective of fully permitting and approving work to construct a frontier AI data center at each site by the end of 2025:

(i) inclusion of sufficient terrain with appropriate land gradients, soil durability, and other topographical characteristics for frontier AI data centers;

(ii) minimized adverse effects from AI infrastructure development or operation on local communities’ health, wellbeing, and resource access; natural

(i) contain completed, permitted, or planned clean generation projects that can enable delivery of electricity as described in this subsection and possess an executed interconnection agreement with a transmission provider;

(ii) have been allocated as available for solar applications in the *Final Programmatic Environmental Impact Statement and Proposed Resource Management Plan Amendments for Utility-Scale Solar Energy Development*, published by BLM, or that have otherwise been allocated as available for clean-energy applications in a BLM resource management plan;

(iii) have reasonable access to and are located nearby existing high-voltage transmission lines that have at least one gigawatt of additional capacity available, or for which such capacity can be reasonably developed through reconductoring, grid-enhancing technologies, or transmission upgrades;

(iv) possess the characteristics described in subsections (a)(i)–(x) of this section, in a manner that is consistent with the objective of fully permitting and approving work to construct utility-scale power facilities on a timeline that allows for the operation of those facilities by the end of 2027 or as soon as feasible thereafter; and

(v) possess other characteristics conducive to enabling new clean power development at such sites to contribute to lower regional electricity prices or to bring other community benefits.

(c) By March 15, 2025, the Secretary of the Interior, acting through the Director of BLM and in consultation with the Secretary of Energy, shall, if possible, designate at least five regions composed of lands or subsurface areas managed by the Department of the Interior as Priority Geothermal Zones (PGZs). The Secretary of the Interior shall designate those regions based on their potential for geothermal power generation resources, including hydrothermal and next-generation geothermal power and thermal storage; diversity of geological characteristics; and possession of the characteristics described in subsections (a)(i)–(x) and (b)(i)–(v) of this section.

(d) The Secretary of Defense, the Secretary of Energy, and the Secretary of the Interior shall each make a legal determination as to whether each site identified pursuant to subsections (a) and (b) of this section is available for lease or for the issuance of a right of way, as appropriate, pursuant to the authority of the Secretary that made the identification, and as to whether the Secretary has the legal authority to lease or grant a right of way over or upon each site identified for the construction of frontier AI infrastructure. For purposes of this order, a site shall be considered “cleared” under this subsection if the relevant Secretary has determined that the site is available for lease and the Secretary concerned has the authority to lease it.

(e) By March 31, 2025, the Secretary of Defense and the Secretary of Energy, in coordination with the heads of any other agencies that either Secretary deems appropriate, shall coordinate to design, launch, and administer competitive public solicitations of proposals from non-Federal entities to lease Federal land to construct frontier AI infrastructure, including frontier AI data centers, on sites identified under subsection (a) of this section and cleared under subsection (d) of this section, if any. When issuing the solicitations, the Secretaries shall announce the sites identified under subsection (a) of this section and cleared under subsection (d) of this section, if any, and additional relevant information including the sites’ geographic coordinates, technical characteristics, proximity to sites identified consistent with subsection (b) of this section and cleared under subsection (d) of this section, if any, and other relevant information. The solicitations shall, to the extent consistent with applicable law and to the extent the Secretaries agree that such requirements promote national defense, national security, or the public interest, as appropriate, require applicants to identify particular sites on which they propose to construct and operate frontier AI infrastructure; submit a detailed plan specifying proposed timelines, financing methods, and technical construction plans associated with such construction

work, including a contingency plan for decommissioning infrastructure on Federal sites; submit a plan that describes proposed frontier AI training work to occur at the site once operational; submit a plan for detailing the extent of the use of high labor and construction standards as described in subsection (g)(viii) of this section; and submit a plan with proposed lab-security measures, including personnel and material access requirements, that could be associated with the operation of frontier AI infrastructure. These requirements should be designed to ensure adequate collection of information from applicants regarding the criteria in subsections (g)(i)–(xvi) of this section. The solicitations shall close within 30 days of their issuance.

(f) By March 31, 2025, the Secretary of the Interior, in consultation with the Secretary of Defense and the Secretary of Energy, shall publicize the sites identified under subsection (b) of this section and cleared under subsection (d) of this section, if any, and additional relevant information including the sites' geographic coordinates, technical characteristics, proximity to sites identified consistent with subsection (a) of this section and cleared under subsection (d) of this section, if any, and other relevant information.

(g) By June 30, 2025, the Secretary of Defense and the Secretary of Energy shall announce any winning proposals identified through solicitations described in subsection (e) of this section. In selecting any winning proposals, the Secretary of Defense and the Secretary of Energy shall, in consultation with each other, assign winners the opportunity to apply for any Federal permits needed to build and operate frontier AI infrastructure pursuant to the frameworks described in subsection (h) of this section on any sites included in the solicitations issued under subsection (e) of this section, as the Secretaries deem appropriate. The Secretaries shall consult with the Attorney General on the implications of selections on the competition and market-structure characteristics of the broader AI ecosystem. The Chair of the Federal Trade Commission is encouraged to participate in these consultations. The Secretaries shall, to the extent consistent with applicable law and to the extent that the Secretaries assess that the requirement promotes national defense, national security, or the public interest, as appropriate, select at least one proposal developed and submitted jointly by a consortium of two or more small- or medium-sized organizations—as determined by those organizations' market capitalization, revenues, or similar characteristics—provided that the Secretaries receive at least one such proposal that meets the appropriate qualifications. The Secretaries shall provide technical assistance, as appropriate, to small- or medium-sized organizations seeking to submit proposals. The criteria for selecting winning proposals shall include, at a minimum, consideration of the following characteristics of the applicants and any identified partner organizations, to the extent consistent with applicable law and to the extent that the Secretaries agree that the listed characteristics promote national defense, national security, or the public interest, as appropriate:

- (i) proposed financing mechanisms and sources of funds secured or likely to be secured for work to be performed at the site;
- (ii) plans for ensuring high-quality AI training operations to be executed at the site by the applicant or third-party partners;
- (iii) plans for maximizing energy, water, and other resource efficiency, including waste-heat utilization in constructing and operating the AI data center at the site, the strength of the proposed energy master plan for the site, and the quality of analysis of potential strains on local communities;
- (iv) safety and security measures, including cybersecurity measures, proposed to be implemented at the site, and capabilities for such implementation;
- (v) capabilities and acumen of applicable AI scientists, engineers, and other workforce essential to the operation of AI infrastructure;

(vi) plans for commercializing or otherwise deploying or advancing deployment of appropriate intellectual property, including AI model weights, developed at the site, as well as plans for commercializing or otherwise deploying or advancing deployment of innovations related to power generation and transmission infrastructure developed in the course of building or operating AI infrastructure;

(vii) plans to help ensure that the construction and operation of AI infrastructure does not increase electricity costs to other ratepayers or water costs to consumers, including, as appropriate, through appropriate proposed or recommended future engagement with any applicable regulatory authorities and State, Tribal, or local governments;

(viii) plans to use high labor standards that help ensure continuous and high-quality work performed on the site, such as paying prevailing wages; hiring registered apprentices; promoting positive labor-management relations through a project labor agreement; and otherwise adopting high job quality and labor standards for the construction and operations workforce as set forth in Executive Order 14126 of September 6, 2024 (Investing in America and Investing in American Workers), and a plan to address labor-related risks associated with the development and use of AI;

(ix) design features and operational controls and plans that mitigate potential environmental effects and implement strong community health, public safety, and environmental protection measures;

(x) other benefits to the community and electric grid infrastructure surrounding the site;

(xi) experience completing comparable construction projects;

(xii) experience in compliance with Federal, State, and local permits and environmental reviews relevant to construction and operation of AI infrastructure or, in the alternative, other evidence of an ability to obtain and comply with such permits or reviews in an efficient manner;

(xiii) the presence of organizational and management structures to help ensure sound governance of work performed at the site;

(xiv) the effect of the selection of an applicant on the emergence of an interoperable, competitive AI ecosystem;

(xv) whether an applicant has already been assigned an opportunity, or is being assigned another opportunity, to build a frontier AI data center on a Federal site through the solicitation process described in this section; and

(xvi) other considerations of national defense, national security, or the public interest, including economic security, as the Secretary of Defense and the Secretary of Energy deem appropriate.

(h) By June 30, 2025, the Secretary of Defense and the Secretary of Energy, in consultation with the Secretary of the Interior, shall each develop a framework through which any winning applicants selected under subsection (g) of this section may apply to lease sites respectively identified under subsection (a) of this section, and cleared under subsection (d) of this section, to construct and operate AI infrastructure, and by which the applicants may own the AI infrastructure facilities on those sites, subject to the conditions described in subsections (i)–(x) of this subsection. To the extent that the Secretaries assess that it is consistent with national defense, national security, or the public interest, as appropriate, these frameworks shall allow for winning applicants to cooperate with other appropriate private-sector entities on construction and operation activities, including through contracting and subcontracting relationships, and the frameworks shall not require that parties proposing to own AI infrastructure be identical to those proposing to operate the infrastructure or perform work at the sites on which the infrastructure is located. Actions taken by Federal entities pursuant to the frameworks shall conform to any applicable requirements of Appendix B of Office of Management and Budget (OMB) Circular A–

11 and any other appropriate budget-scoring practices; applicable in-kind consideration shall be taken into account in calculating the cost to lessees of any such leases. As part of the foregoing work, the Secretary of Defense and the Secretary of Energy shall, to the extent consistent with their respective authorities and with national defense, national security, or the public interest, as appropriate, require lease or contract terms that accomplish the following:

(i) establish a target of the applicant's beginning construction of a frontier AI data center by January 1, 2026, and commencing full-capacity operation of the AI infrastructure by December 31, 2027, subject to fulfillment of relevant statutory and regulatory requirements, and in a manner consistent with opportunities to operate the infrastructure at or below full capacity at an earlier date;

(ii) require that, concurrent with operating a frontier AI data center on a Federal site, non-Federal parties constructing, owning, or operating AI infrastructure have procured sufficient new clean power generation resources with capacity value to meet the frontier AI data center's planned electricity needs, including by providing power that matches the data center's timing of electricity use on an hourly basis and is deliverable to the data center;

(iii) clarify that non-Federal parties bear all responsibility for paying any costs that parties to the frameworks described in subsection (h) of this section, as well as transmission providers or transmission organizations or other entities not party to the contract, incur from work pursuant to it, including costs of work performed by agencies to complete necessary environmental reviews, any costs related to the procurement of clean power generation resources and capacity in accordance with subsection (g)(ii) of this section, any costs of decommissioning AI infrastructure on Federal sites, any costs of developing transmission infrastructure needed to serve a frontier AI data center on a Federal site, and the fair market value of leasing and using applicable Federal lands;

(iv) require adherence to technical standards and guidelines for cyber, supply-chain, and physical security for protecting and controlling any facilities, equipment, devices, systems, data, and other property, including AI model weights, that are developed, acquired, modified, used, or stored at the site or in the course of work performed on the site. The Secretary of Commerce, acting through the Director of the National Institute of Standards and Technology (NIST) and the Director of the AI Safety Institute (AIS) at NIST, in consultation with the Secretary of Defense, the Secretary of Energy, and the Director of National Intelligence, shall identify available standards and guidelines to which adherence shall be required under this subsection. The identified standards should reflect and incorporate guidelines and best practices developed by the Secretary of Commerce, acting through the Director of NIST, pursuant to Executive Order 14028 of May 12, 2021 (Enhancing United States Cybersecurity), and Executive Order 14110 of November 1, 2023 (Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence). The Secretary of Commerce, acting through the Director of AIS at NIST, shall support the ongoing improvement of the framework described in this subsection by developing security guidelines for frontier AI training and operation and, as part of this work, shall comprehensively evaluate the security implications of publicly available AI models that the Secretary of Commerce, acting through the Director of AIS at NIST, deems globally significant;

(v) require that non-Federal parties owning or operating frontier AI data centers sign a memorandum of understanding with the Secretary of Commerce, acting through the Director of AIS at NIST, to facilitate collaborative research and evaluations on AI models developed, acquired, modified, run, or stored at the site or in the course of work performed on the site, for the purpose of assessing the national-security or other significant risks of those models;

(vi) require non-Federal parties to report information about investments or financial capital from any person used or involved in the development (including construction), ownership, or operation of AI infrastructure on the site and in the development, operation, or use of AI models operating in such AI infrastructure, as appropriate to evaluate risks to national security; and require non-Federal parties to limit the involvement in any such activities of, or the use or involvement in any such activities of investments or financial capital from, any person whom the Secretaries of Defense or Energy deem appropriate on national security grounds;

(vii) require non-Federal parties owning or operating AI data centers on Federal sites to take appropriate steps to advance the objective of harnessing AI, with appropriate safeguards, for purposes of national security, military preparedness, and intelligence operations, including with respect to the objectives and work outlined in NSM–25. Such steps shall, as consistent with applicable legal authorities, include collaborating with the Federal Government on regularly recurring assessments of the national-security implications of AI models developed on Federal sites, as appropriate. In addition, as appropriate and consistent with any relevant Federal procurement laws and regulations, the non-Federal parties shall be required to commit to providing access to such models, and critical resources derivative of such models, to the Federal Government for national-security applications at terms at least no less favorable than current market rates, consistent with NSM–25 and the associated Framework to Advance AI Governance and Risk Management in National Security. To the extent feasible, AI models and resources derived from them shall be developed and provided to the Federal Government in a manner that prevents vendor lock-in and supports interoperability, including as consistent with the measures in section 5 of OMB Memorandum M–24–18;

(viii) require that non-Federal parties owning or operating frontier AI data centers on Federal sites develop plans to make available computational resources that are not dedicated to supporting frontier AI training, or otherwise allocated under another provision, for commercial use by startups and small firms on nondiscriminatory terms and in a manner that minimizes barriers to interoperability, entry, or exit for users;

(ix) require non-Federal parties owning or operating AI infrastructure on Federal sites to explore the availability of clean energy resources—such as geothermal power generation resources and thermal storage, long-duration storage paired with clean energy, and carbon capture and sequestration as described in section 3(e) of this order, as well as beneficial uses of waste heat—at any appropriate sites that those parties lease for purposes of constructing frontier AI data centers on Federal sites or procuring power generation capacity to serve these data centers; and

(x) require AI developers owning and operating frontier AI data centers on Federal sites either to procure, for use in the development of their data centers, an appropriate share (as measured by monetary value) of leading-edge logic semiconductors fabricated in the United States to the maximum extent practicable; or to develop and implement a plan, subject to the respective approval of the Secretary of Defense or the Secretary of Energy, to qualify leading-edge logic semiconductors fabricated in the United States for use in the developer's data centers as soon as practicable. The Secretary of Defense and the Secretary of Energy shall develop any such requirements—including any determinations about amounts of leading-edge logic semiconductors that may be considered “appropriate”—in consultation with the Secretary of Commerce.

(i) Within 1 year of the date of this order and consistent with applicable law, the Secretary of Defense, in consultation with the Secretary of Commerce, the Secretary of Energy, the Secretary of Homeland Security, the Director of National Intelligence, and the Assistant to the President for National Security Affairs, shall issue regulations that prescribe heightened safeguards to protect computing hardware acquired, developed, stored, or

used on any sites on which frontier AI infrastructure is located and that are managed by the Department of Defense, as needed to implement or build upon the objectives of, or the requirements established pursuant to, subsection 4(g)(iv). The regulations shall include requirements to conform with appropriate high-impact level standards identified through the Federal Risk and Authorization Management Program, and they shall further provide for appropriate penalties consistent with applicable authorities. No less than annually the Secretary of Defense, in consultation with the aforementioned individuals, shall review the need for updates to the regulations, and promulgate any necessary revisions. The Secretary of Energy shall impose substantively the same requirements with respect to frontier AI infrastructure on sites managed by the Department of Energy, to the extent authorized by law.

(j) To enable the use—for advancing geothermal power development, including the development of thermal storage—of Federal lands already subject to leases:

(i) Within 180 days of the date of this order, the Secretary of the Interior shall establish a program with personnel dedicated to providing technical assistance for, streamlining, and otherwise advancing direct-use leasing of geothermal projects on BLM lands, including as consistent with the policies set forth in 43 C.F.R. subpart 3205, and leases of geothermal projects on lands subject to mining claims or under an oil and gas lease.

(ii) When issuing leases and related authorizations for geothermal projects, the Secretary of the Interior shall consider the extent to which the requirements of the National Environmental Policy Act (NEPA), 42 U.S.C. 4321 *et seq.*, the Endangered Species Act, 16 U.S.C. 1531 *et seq.*, and other appropriate statutes have been satisfied by prior analyses of the lease area.

(k) In performing the work described in section 4 of this order, including as related to the selection and management of sites, the head of each respective Federal agency shall:

(i) consult, as appropriate and consistent with applicable law, Executive Order 13175 of November 6, 2000 (Consultation and Coordination with Indian Tribal Governments), and the Presidential Memorandum of November 30, 2022 (Uniform Standards for Tribal Consultation), with Tribal Nations for which such work may have implications or who otherwise request such consultation;

(ii) seek input from, as appropriate and consistent with applicable law and Administration policies, with State and local governments and other stakeholders and communities for which such work may have implications; and

(iii) consider taking actions that present the greatest opportunities to support the goals described in *Safely and Responsibly Expanding U.S. Nuclear Energy: Deployment Targets and A Framework for Action* (November 2024).

Sec. 5. Protecting American Consumers and Communities. (a) Within 180 days of the date of this order, the Secretary of Energy, in consultation with the Chair of the Council of Economic Advisors and the heads of other agencies that the Secretary deems appropriate, shall submit a report to the President on the potential effects of AI data centers on electricity prices for consumers and businesses. This report shall include electricity-rate-structure best practices for appropriate Federal agencies, State regulators, and transmission providers and transmission organizations to promote procurement of clean energy generation resources as components of AI infrastructure without increasing costs for other customers through cost-allocation processes or other mechanisms—particularly in regions that have or are expected to have high concentrations of AI infrastructure—as well as regional analyses of key data center hubs. The report shall further account for any existing approaches developed by Federal agencies to engage transmission providers and State regulators regarding electricity prices. After submitting the report, the Secretary of Energy shall engage appropriate private-sector

entities, to include the winning applicants selected under subsection 4(g) of this order, on the report's findings and recommendations.

(b) The Secretary of Energy shall provide technical assistance to State public utility commissions to consider rate structures, including clean transition tariffs and any other appropriate structures identified under subsection (a) of this section, to enable new AI infrastructure to use clean energy without causing unnecessary increases in electricity or water prices.

(c) The Secretary of Energy and the heads of other appropriate agencies as the Secretary of Energy deems appropriate, shall coordinate to expand research-and-development efforts related to AI data center efficiency. Supported research and development shall cover, as appropriate, efficiency considerations associated with data center buildings, including the data center shell; electrical systems; heating, ventilation, and cooling infrastructure; software; and beneficial use cases for wastewater heat from data center operations. As part of this work, the Secretary of Commerce and the Secretary of Energy shall submit a report to the President identifying appropriate ways that agencies can advance industry-wide data center energy efficiency through research and development, including server consolidation; hardware efficiency; virtualization; optimized cooling and airflow management; and power management, monitoring, and capacity planning.

(d) In implementing this order with respect to AI infrastructure on Federal sites, the heads of relevant agencies shall prioritize taking appropriate measures to keep electricity costs low for households, consumers, and businesses.

(e) Within 180 days of the date of this order, the Director of OMB, in consultation with the Chair of the Council on Environmental Quality (CEQ), shall evaluate best practices for public participation and governmental engagement in the development of potential siting and energy-related infrastructure for data centers, to include practices for seeking input on potential health, safety, and environmental impacts and mitigation measures for nearby communities. The Director shall present recommendations to the Secretary of Defense and the Secretary of Energy, who shall—as feasible and appropriate, and to advance the goals of assuring effective governmental engagement and meaningful public participation—implement and incorporate these recommendations into their siting and related decision-making processes regarding AI infrastructure.

Sec. 6. *Facilitating Electric Grid Interconnections for Federal Sites.* (a) Within 60 days of the date of this order, for the purpose of supporting any winning applicants of the solicitations described in subsection 4(e) of this order, the Secretary of Energy shall establish requirements for transmission providers and transmission organizations to report to the Secretary information regarding surplus interconnection service; available transmission capacity for interconnecting generators; opportunities for clean repowering; and proposed, planned, or initiated projects to build clean power generation capacity for which construction is not complete, but which have executed generation interconnection agreements. Information requested regarding these proposed, planned, or initiated projects shall include the size, location, and generation technology for each such clean power generation project, as well as the status and estimated cost of any transmission upgrades necessary to enable that project's interconnection consistent with the interconnection agreement. The Secretary shall facilitate communication, as appropriate, among the owners of such surplus interconnection service, facilities with opportunities for clean repowering, or clean power generator projects and winning applicants to the solicitations described in subsection 4(e) of this order. The Secretary shall further establish appropriate requirements for transmission providers and transmission organizations to continue reporting information described in this subsection on an ongoing basis, and in any event no less than annually.

(b) Within 120 days of the date of this order, the Secretary of Energy shall identify and communicate, as appropriate, a prioritized list of underutilized points of interconnection that are relevant to AI infrastructure on Federal sites and that demonstrate the highest potential for uses associated

with AI infrastructure. In developing this list, the Secretary shall direct transmission providers and transmission organizations to identify areas of the transmission network best suited to serve as points of interconnection for either data centers or other AI infrastructure that will use electricity from the transmission system—and locations best suited for interconnection of clean generators to serve such data centers—considering criteria such as minimizing the need for transmission upgrades necessary to accommodate such interconnection and access to clean energy generation resources.

(c) By June 30, 2025, the Secretary of Energy, in coordination with the Secretary of Defense and in consultation, as appropriate, with the Secretary of the Interior and the Secretary of Agriculture, shall engage with transmission providers and transmission organizations owning, operating, or maintaining transmission infrastructure located near Federal sites selected for AI infrastructure to identify any grid upgrades, deployment of advanced transmission technologies such as high-performance conductors or grid-enhancing technologies, operational changes, or other steps expected to be required for extending interconnection services to AI infrastructure by the end of 2027. Such engagements shall continue as the parties deem appropriate, and they shall prioritize, as appropriate, efforts to enable use of surplus interconnection services, clean repowering, and other methods of accelerated shifts toward clean power and beneficial use of waste heat. The engagements shall also include consideration of ways that the performance of such work as described in this subsection can most contribute to lower regional electricity prices.

(d) The Secretary of Energy shall conduct an analysis of currently available transmission infrastructure serving potential sites, and the likely cost and feasibility of, and timeline for, developing additional such infrastructure needed for constructing and operating a frontier AI data center on sites identified under subsection 4(a) of this order, and cleared under subsection 4(d) of this order, including by providing the frontier AI data center with clean energy and capacity. The Secretary shall identify and collect from transmission providers and transmission organizations information that the Secretary deems necessary for the analysis required under this subsection. The Secretary shall, as appropriate, treat such information as critical electric infrastructure information.

Sec. 7. *Expeditionously Processing Permits for Federal Sites.* (a) The heads of Federal Permitting Agencies shall prioritize work and exercise all applicable authorities, as appropriate, to expedite the processing of permits and approvals required for the construction and operation of AI infrastructure on Federal sites, with the goal of issuing all permits and approvals required for construction by the end of 2025 or as soon as they can be completed consistent with applicable law. As part of this work, the Permitting Council may provide coordination of permitting for AI infrastructure on Federal sites, as appropriate and to the extent that the relevant developers of AI infrastructure submit a notice of the initiation of a proposed covered project under 42 U.S.C. 4370m–2 and the project is determined to be such a covered project by the Permitting Council.

(b) To facilitate expeditious implementation of the requirements under NEPA with respect to Federal sites:

(i) The Secretary of Defense, the Secretary of the Interior, and the Secretary of Energy shall identify, within their respective agencies, personnel dedicated to performing NEPA reviews of projects to construct and operate AI infrastructure on Federal sites.

(ii) The Secretary of Defense, in consultation with the Secretary of the Interior, the Secretary of Agriculture, the Secretary of Commerce, and the Secretary of Energy, shall undertake a programmatic environmental review, on a thematic basis, of the environmental effects—and opportunities to mitigate those effects—involved with the construction and operation of AI data centers, as well as of other components of AI infrastructure as the Secretary of Defense deems appropriate. The review shall conclude, with all appropriate documents published, on the date of the close of

the solicitations described in subsection 4(e) of this order, or as soon thereafter as possible. The review shall, as applicable, incorporate by reference previously developed environmental studies, surveys, and impact analyses, including the analysis described in subsection 4(b)(ii) of this order.

(iii) After the conclusion of the programmatic review described in subsection (b)(ii) of this section, the Secretary of Defense, the Secretary of the Interior, the Secretary of Energy, and the heads of other relevant agencies, as appropriate, shall commence any further environmental reviews that are required under NEPA for the construction and operation of AI infrastructure on Federal sites, including by applying any available categorical exclusions. Such reviews shall, as appropriate, build on or incorporate by reference the programmatic environmental review conducted under subsection (b)(ii) of this section, as well as any other studies, surveys, and impact analyses that the Secretaries deem appropriate.

(c) To advance expeditious preconstruction permitting and ensure full compliance with air-quality permit requirements for AI infrastructure, the Administrator of the EPA, in consultation with the Secretary of Defense and the Secretary of Energy, shall:

(i) within 30 days of the selection of winning applications under subsection 4(g) of this order, engage State and local permitting authorities with jurisdiction over sites selected for AI infrastructure, as appropriate, to enhance relevant authorities' understanding of the technical characteristics of AI infrastructure projects as relevant to new source reviews under the Clean Air Act, 42 U.S.C. 7401 *et seq.*, and to enhance the public's understanding of the same, as well as to facilitate the acquisition of information by AI developers operating on Federal sites regarding best practices for expeditiously obtaining air-quality permits;

(ii) continue engagements with State and local permitting authorities, and provide technical assistance to AI developers operating on Federal sites, on an ongoing basis and as appropriate, to help advance expeditious conclusion of, and compliance with, new source reviews; and

(iii) following the acquisition of all preconstruction air-quality permits by developers, take steps to ensure, on an ongoing basis and as appropriate, that AI developers operating on Federal sites adhere to all requirements of operational air-quality permits applicable to their respective projects; that information needed to demonstrate compliance, possibly including air-monitoring data, is made publicly available and regularly updated; and that best practices are identified for air-emissions reduction and air-quality monitoring regarding AI infrastructure on Federal sites.

(d) To help ensure expeditious permitting or permission processes related to waters of the United States and harbor and river improvements, the Secretary of Defense shall prioritize work, as appropriate, to process applications for permits administered by the United States Army Corps of Engineers (USACE) under the Clean Water Act, 33 U.S.C. 1251 *et seq.*, and to process applications for permission for appropriate projects under section 14 of the Act of March 3, 1899 (33 U.S.C. 408), as consistent with the statutes' requirements, in order to render determinations on any such permits or permissions associated with AI infrastructure on Federal sites by the end of 2025, or as soon as feasible consistent with statutory requirements. The Secretary shall, consistent with applicable law, prioritize allocation of resources toward USACE district offices, and direct the allocation of resources within such offices, as needed to comply with this directive. The Secretary shall further apply all general permits applicable to AI infrastructure where appropriate to promote expeditious permitting on such Federal sites.

(e) Within 30 days of the selection of any winning applications under subsection 4(g) of this order, the Secretary of Defense and the Secretary of Energy shall initiate Tribal consultations as applicable and appropriate based on the sites selected. Upon receipt of sufficient project information, the Secretary of Defense and the Secretary of Energy shall further initiate

consultations with the Secretary of the Interior, acting through the Director of the United States Fish and Wildlife Service (USFWS), to ensure that the construction and operation of AI infrastructure on each site that is identified under subsection 4(a) of this order, cleared under subsection 4(d) of this order, and subsequently chosen as the location for the construction and operation of AI infrastructure pursuant to a winning application under subsection 4(g) of this order are not likely to jeopardize the continued existence of any endangered species or threatened species or result in the destruction or adverse modification of a critical habitat of such species. The Secretary of Defense and the Secretary of Energy shall conclude such consultations with USFWS, to the maximum extent practicable, within 90 days of the initiation of such consultations when feasible and consistent with statutory requirements.

(f) To advance the development of geothermal energy production and thermal storage, including in support of AI infrastructure on Federal sites:

(i) Within 60 days of the date of this order, the Secretary of the Interior shall undertake a programmatic environmental review, on a thematic basis, of the environmental impacts and associated mitigations involved with the construction and operation of a geothermal power plant.

(ii) By the date on which the review described in subsection (f)(i) of this section is completed, the Secretary of the Interior shall establish a target cumulative capacity of permitted or operational geothermal projects by a year that the Secretary shall designate.

(iii) Within 60 days of the date of this order, the Secretary of the Interior shall assess existing categorical exclusions that are listed in the NEPA procedures of other agencies and could apply to actions taken in connection with geothermal energy development. The Secretary shall propose adopting such categorical exclusions as the Secretary, after consultation with the heads of agencies whose NEPA procedures list the categorical exclusions, deems appropriate, and, after considering all comments received through applicable public comment processes, take any actions to adopt categorical exclusions that are appropriate given the received comments, as consistent with the requirements of NEPA and 40 C.F.R. parts 1500–1508. The Secretary shall prioritize the expeditious permitting of geothermal projects, including the application of any appropriate categorical exclusions adopted under this subsection, on PGZs. The Secretary shall prioritize work to expeditiously permit geothermal projects on PGZs above the work described in subsection (f)(i) of this section.

(iv) When issuing leases and related authorizations for geothermal projects on PGZs, the Secretary of the Interior shall fulfill the requirements of NEPA and the Endangered Species Act in a manner that allows for the earliest possible operation of geothermal power plants consistent with applicable law.

(v) The Secretary of Defense, the Secretary of the Interior, and the Secretary of Energy shall, as appropriate, coordinate to determine and clarify appropriate procedures for the execution of leases or subleases for developing or expanding clean energy generation resources, including geothermal energy generation resources, on withdrawn lands subject to the jurisdiction of the Department of Defense or the Department of Energy.

Sec. 8. *Ensuring Adequate Transmission Infrastructure for Federal Sites.*

(a) The Secretary of Energy, in consultation with the Secretary of Defense and the Secretary of the Interior, shall take steps to enable AI infrastructure on Federal sites to have reliable access to transmission facilities adequate for the operation of frontier AI data centers by the end of 2027.

(b) To promote any needed upgrades and development of transmission infrastructure that is located on or that is necessary to support Federal sites with AI infrastructure, the Secretary of Energy, in consultation with the Secretary of the Interior, acting through the Director of BLM and the Director of USFWS, shall:

- (i) by September 30, 2025, identify and initiate use of all appropriate authorities to construct, finance, facilitate, and plan such upgrades and development, including through the Transmission Infrastructure Program administered by the Western Area Power Administration; and
 - (ii) prioritize the allocation of staff and resources for developing transmission infrastructure needed to support AI infrastructure on Federal sites—and in doing so, as appropriate, allocate relevant staff and resources from any component within the Department of Energy for this purpose—consistent with the requirements and objectives of this order and applicable law.
- (c) Because of the importance of frontier AI infrastructure, including transmission capacity, to the defense industrial base, critical infrastructure, and military preparedness:
- (i) The Secretary of Energy shall consider expected use of frontier AI data centers on Federal sites as part of the Secretary's triennial study of electric transmission capacity constraints and congestion under section 216(a)(1) of the Federal Power Act (16 U.S.C. 824p(a)(1)).
 - (ii) Consistent with the requirements of section 216(a)(2) of the Federal Power Act (16 U.S.C. 824p(a)(2)), and based on any findings made in future studies of electric transmission capacity constraints and congestion as described in subsection (c)(i) of this section, the Secretary shall consider whether to designate geographic areas around frontier AI infrastructure on Federal sites as national interest electric transmission corridors.
- (d) The Secretary of Energy shall, as appropriate, help ensure that transmission facilities upgraded or developed to support AI data centers on Federal sites:
- (i) are designed to support all reasonably foreseeable electric loads, including through the deployment of grid-enhancing technologies, high-performance conductors, and other advanced transmission technologies, including those described in the Department of Energy's *Innovative Grid Deployment* Liftoff report, that will increase the capabilities of the transmission facilities on a timely and cost-effective basis; and
 - (ii) conform to conductor efficiency standards or other technical standards or criteria that the Secretary determines will optimize facilities' performance and cost-effectiveness.
- (e) To improve the timely availability of critical grid equipment for frontier AI infrastructure, such as electrical transformers, circuit breakers, switchgears, and cables, and to protect electricity consumers from exposure to rising equipment prices:
- (i) Within 90 days of the date of this order, the Secretary of Defense, the Secretary of Commerce, and the Secretary of Energy shall jointly consult with domestic suppliers of such technologies on the expected needs of AI infrastructure on Federal sites, suppliers' current production plans, and opportunities for Government support in helping suppliers meet market demands.
 - (ii) Within 180 days of the date of this order, the Secretary of Energy shall facilitate industry-led convenings on transformers and other critical grid components, which shall include appropriate representatives from agencies, transmission providers and transmission organizations, domestic suppliers of transformers, data center developers, and other private-sector organizations. On an ongoing basis, the Secretary, after consulting with participants in the industry-led convenings, shall:
 - (A) on at least an annual basis, develop and publish supply and demand forecasts for transformers, including forecasts for different transformer variants and analyses of supply and demand trends under different future scenarios, which shall include scenarios for growth in electricity demand from AI infrastructure and other sources of demand; and

(B) consider and, as appropriate, execute purchases of transformers and other critical grid components in order to provide demand certainty for domestic manufacturers to invest in capacity for meeting the needs of AI infrastructure. Any decision to execute such purchases shall be based on economic or other industry data, including the capacity utilization of domestic suppliers of transformers or other components, that the Secretary deems relevant to evaluating the status of the domestic industry. The Secretary shall subsequently execute sales of any purchased transformers or other critical grid components at times that the Secretary deems appropriate based on such data.

(f) Within 180 days of the date of this order, the Secretary of Energy shall establish requirements for transmission providers and transmission organizations to report to the Secretary transmission-related information to assist in siting and accelerating the interconnection of generation resources to serve frontier AI data centers on sites identified under section 4(a) of this order and cleared under subsection 4(d) of this order. Such information may include data on transmission congestion to help identify where additional transmission investments could enable the development of additional transmission capacity to serve such AI data centers.

(g) Within 180 days of the date of this order, the heads of agencies that possess loan or loan-guarantee authorities shall evaluate whether any such authorities could be used to support the development of AI infrastructure on Federal sites—including the production of critical grid equipment as described in subsection (e) of this section, or other actions to strengthen the AI infrastructure supply chain. In cases in which any authorities are available and appropriate for this purpose, the heads of relevant agencies shall provide that information to developers of AI infrastructure on Federal sites or other appropriate private-sector entities.

Sec. 9. Additional Efforts to Improve Permitting and Power Procurement Nationwide. (a) The heads of Federal Permitting Agencies shall designate, with respect to each of their component agencies, dedicated staff to handle all matters related to permits and approvals for AI infrastructure. Such designations shall include personnel dedicated to coordinating with and addressing the needs of applicants for permits under the respective agency's purview. In designating such personnel, the heads of Federal Permitting Agencies shall, as appropriate, implement staffing arrangements and other mechanisms that accelerate permitting for AI infrastructure to the maximum extent possible.

(b) To improve review practices pursuant to NEPA:

(i) Within 60 days of the date of this order, the heads of Federal Permitting Agencies, in coordination with the Chair of CEQ, shall assess existing categorical exclusions and identify opportunities to establish new categorical exclusions to support AI infrastructure on Federal sites, consistent with the requirements of NEPA and 40 C.F.R. parts 1500–1508. The heads of agencies whose NEPA regulations include categorical exclusions related to fiber-optic cables are encouraged, in undertaking these assessments, to evaluate whether such categorical exclusions may be applied to the development of fiber-optic cables as used for AI infrastructure.

(ii) Within 120 days of the date of this order, the heads of Federal Permitting Agencies shall, as appropriate and consistent with applicable law, propose any new categorical exclusions and, after considering all comments received through applicable public comment processes, take any actions to establish categorical exclusions that are appropriate given the received comments.

(iii) Within 120 days of the date of this order, and consistent with the directives described in section 7 of this order, the Secretary of Defense, the Secretary of the Interior, the Secretary of Agriculture, and the Secretary of Energy shall identify any existing categorical exclusions that are listed in the NEPA procedures of other agencies and that are relevant to the development of clean energy, electric transmission, or AI data centers

and take any appropriate steps to adopt such categorical exclusions where appropriate and consistent with the requirements of NEPA and 40 C.F.R. parts 1500–1508. The Secretary of Defense, the Secretary of the Interior, the Secretary of Agriculture, and the Secretary of Energy shall take any appropriate steps to adopt and apply such categorical exclusions to AI infrastructure on Federal sites where consistent with the requirements of NEPA and 40 C.F.R. parts 1500–1508.

(c) Within 180 days of the date of this order, the Secretary of Energy shall issue a request for information on opportunities for accelerated interconnection at existing power plants, including as related to surplus interconnection service and clean repowering. The request shall seek details on the ownership of such plants with surplus interconnection service and the plants' suitability for colocation of new clean power generation resources with shared grid access.

(d) Within 90 days of the date of this order, the Secretary of Energy shall issue a request for information from private-sector entities including transmission providers, transmission organizations, and clean energy developers regarding load interconnection processes. The Secretary shall subsequently engage with transmission providers and transmission organizations regarding best practices to improve the transparency and efficiency of such processes, including through adopting new technologies, software, and procedures. The Secretary shall provide technical assistance and financial assistance to facilitate such adoption, as appropriate. The Secretary shall publish a report describing the results of this work within 1 year of the date of this order.

(e) To promote the expeditious, responsible development of nuclear power generation resources, the Secretary of Defense and the Secretary of Energy shall:

(i) seek to facilitate the deployment of additional nuclear power and, as relevant, supply-chain services on lands owned by, respectively, the Department of Defense and the Department of Energy—including Department of Defense installations and sites owned or managed by the Department of Energy National Laboratories—by, as appropriate and consistent with applicable law, identifying opportunities for such deployment on specific lands to the extent such opportunities exist and, in the case of the Secretary of Energy only, by evaluating whether financial support for such deployment is appropriate;

(ii) within 180 days of the date of this order, coordinate to publish a joint list of ten high-priority sites—or, if fewer than ten appropriate sites exist, as many sites as possible—which may overlap with sites identified and cleared under section 4 of this order, that are most conducive to expeditious, safe, and responsible deployment of additional nuclear power capacity readily available to serve AI data center electricity demand by December 31, 2035, taking into account factors including Federal, State, Tribal, and local ordinances; permitting and other regulatory requirements; water access; climate resilience and natural-hazard risks; and transmission and interconnection dynamics; and

(iii) within 1 year of the date of this order, publish either a joint plan or their own respective plans describing how each Secretary will facilitate deployment of additional nuclear power capacity as described in this subsection on any such sites. Any such plan shall address selection of appropriate nuclear reactor technologies; the licensing and permitting of relevant technologies or facilities; the approach that each Secretary would take to ensure the safe and responsible transportation of uranium and any other radioactive material to the site; the approach that each Secretary would take to ensure the safe and responsible storage or disposal of any spent nuclear fuel; remediation of the site after the plant ceases operation as needed; and any other steps necessary to ensure the deployment will protect public health, safety, and the environment, consistent with all applicable legal requirements and the principles of the document

entitled *Safely and Responsibly Expanding U.S. Nuclear Energy: Deployment Targets and a Framework for Action* (November 2024); and

(iv) when carrying out actions under this subsection, comply with the directives of section 4(k) of this order.

(f) Within 180 days of the date of this order, the Secretary of Commerce, in consultation with the Secretary of Defense, the Secretary of Energy, and the White House Council on Supply Chain Resilience, shall submit a report to the President on supply chain risks applicable to the United States data center industry. The report shall include analysis of supply chain risks associated with the materials used to construct and maintain data centers, the electronics necessary to operate a data center, and emerging data center technologies, as well as recommended steps for the Federal Government to take to address identified risks. The report shall also include analysis on supply chain risks applicable to the generation and transmission infrastructure needed to power AI data centers. On an ongoing basis, as appropriate, the Secretary of Commerce shall engage with the private sector to identify emerging supply chain risks that have the potential to undermine the success of the United States AI infrastructure industry—with such success defined to include the industry's commercialization of emerging technologies—and to recommend policy solutions to address identified risks.

(g) Within 180 days of the date of this order, to promote the expeditious, responsible development and deployment of distributed energy solutions that support the development and operation of AI infrastructure, the Secretary of Energy shall develop model contracts for using distributed energy resources (DERs) to increase the local grid's capacity to support AI infrastructure. In developing such contracts, the Secretary shall consider options for cost-effective uses of DERs, including distribution-sited generation resources, energy storage assets, and opportunities for flexible management of electricity demand. The model contracts shall, as appropriate, include clauses providing for the owners of data centers to finance costs incurred by other entities in developing, installing, and operating DERs, consistent with the objective of utilities accounting for these financing activities when processing data center owners' interconnection applications.

(h) By July 31, 2025, the Permitting Council shall engage with developers of AI infrastructure to advance their understanding of resources available under title 41 of the Fixing America's Surface Transportation Act (Public Law 114–94) to accelerate permitting processes and reviews for clean energy projects that are part of AI infrastructure on Federal sites. As part of this work, the Permitting Council, in consultation with the White House Task Force on AI Datacenter Infrastructure announced on October 29, 2024, shall endeavor to engage small developers of AI infrastructure.

(i) Within 180 days of the date of this order, the Secretary of the Army, acting through the Chief of Engineers and Commanding General of the USACE, shall, consistent with applicable law, assess existing nationwide permits (NWP) to determine how they may be applied to facilitate the construction of AI data centers and develop and publish a list of NWPs that could facilitate such construction. The Secretary of the Army, acting through the Chief of Engineers and Commanding General of the USACE, shall, as appropriate and consistent with applicable law, subsequently establish such new NWPs as expeditiously as possible.

(j) Within 60 days of the date of this order, the Secretary of Energy shall release for public comment draft reporting requirements for AI data centers covering all phases of AI data centers' development and operation—including material extraction, component fabrication, transportation, construction, operation, recycling, and retirement—regarding embodied greenhouse gas emissions, water usage, and excess heat or energy expenditures, as distinct from operational intensity of greenhouse gas emissions.

(k) Within 60 days of the date of this order, the Secretary of Energy, in coordination with the Administrator of the EPA and the Chair of CEQ,

shall establish a grand challenge, serving as a call to voluntary action for appropriate private-sector and other stakeholders, for the purpose of:

- (i) setting targets for minimizing the power usage effectiveness ratio and water usage effectiveness ratio of AI data centers, with a goal of bringing the power usage effectiveness ratio of AI data centers on Federal sites below 1.1;
- (ii) promoting best practices for the beneficial use of waste heat and other efforts to maximize efficiency;
- (iii) promoting best practices for data center energy management and sustainable design and operational practices for data centers that avoid or reduce adverse effects on natural and cultural resources and communities, and that protect public health and the environment;
- (iv) raising AI developer and user awareness regarding the comparative energy intensities of different computational tasks; and
- (v) developing best practices and standards for software and algorithmic efficiency.

Sec. 10. *Engagement Abroad.* (a) Within 90 days of the date of this order, the Secretary of State, in consultation with the Secretary of Defense, the Secretary of Commerce, the Secretary of Energy, the Administrator of the United States Agency for International Development, the Assistant to the President for National Security Affairs, and the heads of other relevant agencies as the Secretary of State may deem appropriate, shall develop a plan for engaging allies and partners on accelerating the buildout of trusted AI infrastructure around the world. Such a plan shall include measures to advance collaboration on the global buildout of trusted AI infrastructure; mitigate and prevent harms to local and affected communities; engage the private sector and investor community to identify and mitigate barriers to AI infrastructure investments; support the deployment of commercially available reliable clean power sources and the development and commercialization of emerging clean energy technologies, such as small modular nuclear reactors; exchange best practices for permitting, power procurement, and cultivating talent to build, operate, and maintain trusted AI infrastructure; and strengthen cyber, physical, and supply chain security safeguards related to AI infrastructure. Within 1 year of the date of this order, the Secretary of State shall submit to the Assistant to the President for National Security Affairs a report on actions taken pursuant to this plan.

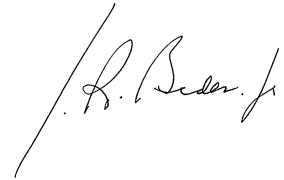
(b) Within 120 days of the date of this order, the Assistant to the President for National Security Affairs shall convene heads of appropriate agencies, to include the Secretary of State, the Secretary of the Treasury, the Secretary of Commerce, the Secretary of Energy, the Chief Executive Officer of the United States International Development Finance Corporation, and the President of the Export-Import Bank of the United States, to identify and implement actions to facilitate United States exports and engagements abroad related to advanced nuclear technologies and relevant supply-chain services.

Sec. 11. *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.



THE WHITE HOUSE,
January 14, 2025.

Presidential Documents

Executive Order 14144 of January 16, 2025

Strengthening and Promoting Innovation in the Nation's Cybersecurity

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the International Emergency Economic Powers Act (50 U.S.C. 1701 *et seq.*), the National Emergencies Act (50 U.S.C. 1601 *et seq.*), section 212(f) of the Immigration and Nationality Act of 1952 (8 U.S.C. 1182(f)), and section 301 of title 3, United States Code, it is hereby ordered as follows:

Section 1. *Policy.* Adversarial countries and criminals continue to conduct cyber campaigns targeting the United States and Americans, with the People's Republic of China presenting the most active and persistent cyber threat to United States Government, private sector, and critical infrastructure networks. These campaigns disrupt the delivery of critical services across the Nation, cost billions of dollars, and undermine Americans' security and privacy. More must be done to improve the Nation's cybersecurity against these threats.

Building on the foundational steps I directed in Executive Order 14028 of May 12, 2021 (Improving the Nation's Cybersecurity), and the initiatives detailed in the National Cybersecurity Strategy, I am ordering additional actions to improve our Nation's cybersecurity, focusing on defending our digital infrastructure, securing the services and capabilities most vital to the digital domain, and building our capability to address key threats, including those from the People's Republic of China. Improving accountability for software and cloud service providers, strengthening the security of Federal communications and identity management systems, and promoting innovative developments and the use of emerging technologies for cybersecurity across executive departments and agencies (agencies) and with the private sector are especially critical to improvement of the Nation's cybersecurity.

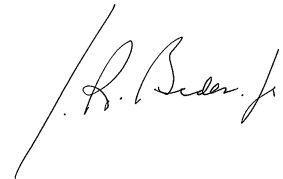
Sec. 2. *Operationalizing Transparency and Security in Third-Party Software Supply Chains.* (a) The Federal Government and our Nation's critical infrastructure rely on software providers. Yet insecure software remains a challenge for both providers and users and makes Federal Government and critical infrastructure systems vulnerable to malicious cyber incidents. The Federal Government must continue to adopt secure software acquisition practices and take steps so that software providers use secure software development practices to reduce the number and severity of vulnerabilities in software they produce.

(b) Executive Order 14028 directed actions to improve the security and integrity of software critical to the Federal Government's ability to function. Executive Order 14028 directed the development of guidance on secure software development practices and on generating and providing evidence in the form of artifacts—computer records or data that are generated manually or by automated means—that demonstrate compliance with those practices. Additionally, it directed the Director of the Office of Management and Budget (OMB) to require agencies to use only software from providers that attest to using those secure software development practices. In some instances, providers of software to the Federal Government commit to following cybersecurity practices, yet do not fix well-known exploitable vulnerabilities in their software, which puts the Government at risk of compromise. The

(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.



THE WHITE HOUSE,
January 3, 2025.

Presidential Documents

Executive Order 14138 of January 3, 2025

Providing an Order of Succession Within the Office of Management and Budget

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the Federal Vacancies Reform Act of 1998, as amended, 5 U.S.C. 3345 *et seq.* (the “Act”), it is hereby ordered that:

Section 1. *Order of Succession.* Subject to the provisions of section 2 of this order, and to the limitations set forth in the Act, the following officials of the Office of Management and Budget, in the order listed, shall act as and perform the functions and duties of the office of Director of the Office of Management and Budget (Director) during any period in which both the Director and the Deputy Director of the Office of Management and Budget have died, resigned, or otherwise become unable to perform the functions and duties of the office of Director:

- (a) Deputy Director for Management;
- (b) Executive Associate Director;
- (c) Associate Director (National Security Programs);
- (d) Associate Director (General Government Programs);
- (e) Associate Director (Education, Income Maintenance, and Labor Programs);
- (f) Associate Director (Health Programs);
- (g) Associate Director (Climate, Energy, Environment, and Science Programs);
- (h) General Counsel;
- (i) Administrator for Federal Procurement Policy;
- (j) Administrator of the Office of Information and Regulatory Affairs;
- (k) Controller, Office of Federal Financial Management; and
- (l) Administrator of the Office of Electronic Government.

Sec. 2. *Exceptions.* (a) No individual who is serving in an office listed in section 1(a)–(l) of this order in an acting capacity shall, by virtue of so serving, act as Director pursuant to this order.

(b) No individual who is serving in an office listed in section 1(a)–(l) of this order shall act as Director unless that individual is otherwise eligible to so serve under the Act.

(c) Notwithstanding the provisions of this order, the President retains discretion, to the extent permitted by law, to depart from this order in designating an acting Director.

Sec. 3. *Revocation.* Executive Order 13615 of May 21, 2012 (Providing an Order of Succession Within the Office of Management and Budget), is hereby revoked.

Sec. 4. *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

Federal Government needs to adopt more rigorous third-party risk management practices and greater assurance that software providers that support critical Government services are following the practices to which they attest.

(i) Within 30 days of the date of this order, the Director of OMB, in consultation with the Secretary of Commerce, acting through the Director of the National Institute of Standards and Technology (NIST), and the Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency (CISA), shall recommend to the Federal Acquisition Regulatory Council (FAR Council) contract language requiring software providers to submit to CISA through CISA's Repository for Software Attestation and Artifacts (RSAA):

(A) machine-readable secure software development attestations;

(B) high-level artifacts to validate those attestations; and

(C) a list of the providers' Federal Civilian Executive Branch (FCEB) agency software customers.

(ii) Within 120 days of the receipt of the recommendations described in subsection (b)(i) of this section, the FAR Council shall review the recommendations and, as appropriate and consistent with applicable law, the Secretary of Defense, the Administrator of General Services, and the Administrator of the National Aeronautics and Space Administration (the agency members of the FAR Council) shall jointly take steps to amend the Federal Acquisition Regulation (FAR) to implement those recommendations. The agency members of the FAR Council are strongly encouraged to consider issuing an interim final rule, as appropriate and consistent with applicable law.

(iii) Within 60 days of the date of the issuance of the recommendations described in subsection (b)(i) of this section, the Secretary of Homeland Security, acting through the Director of CISA, shall evaluate emerging methods of generating, receiving, and verifying machine-readable secure software development attestations and artifacts and, as appropriate, shall provide guidance for software providers on submitting them to CISA's RSAA website, including a common data schema and format.

(iv) Within 30 days of the date of any amendments to the FAR described in subsection (b)(ii) of this section, the Secretary of Homeland Security, acting through the Director of CISA, shall develop a program to centrally verify the completeness of all attestation forms. CISA shall continuously validate a sample of the complete attestations using high-level artifacts in the RSAA.

(v) If CISA finds that attestations are incomplete or artifacts are insufficient for validating the attestations, the Director of CISA shall notify the software provider and the contracting agency. The Director of CISA shall provide a process for the software provider to respond to CISA's initial determination and shall duly consider the response.

(vi) For attestations that undergo validation, the Director of CISA shall inform the National Cyber Director, who shall publicly post the results, identifying the software providers and software version. The National Cyber Director is encouraged to refer attestations that fail validation to the Attorney General for action as appropriate.

(c) Secure software development practices are not sufficient to address the potential for cyber incidents from resourced and determined nation-state actors. To mitigate the risk of such incidents occurring, software providers must also address how software is delivered and the security of the software itself. The Federal Government must identify a coordinated set of practical and effective security practices to require when it procures software.

(i) Within 60 days of the date of this order, the Secretary of Commerce, acting through the Director of NIST, shall establish a consortium with industry at the National Cybersecurity Center of Excellence to develop

guidance, informed by the consortium as appropriate, that demonstrates the implementation of secure software development, security, and operations practices based on NIST Special Publication 800–218 (*Secure Software Development Framework* (SSDF)).

(ii) Within 90 days of the date of this order, the Secretary of Commerce, acting through the Director of NIST, shall update NIST Special Publication 800–53 (*Security and Privacy Controls for Information Systems and Organizations*) to provide guidance on how to securely and reliably deploy patches and updates.

(iii) Within 180 days of the date of this order, the Secretary of Commerce, acting through the Director of NIST, in consultation with the heads of such agencies as the Director of NIST deems appropriate, shall develop and publish a preliminary update to the SSDF. This update shall include practices, procedures, controls, and implementation examples regarding the secure and reliable development and delivery of software as well as the security of the software itself. Within 120 days of publishing the preliminary update, the Secretary of Commerce, acting through the Director of NIST, shall publish a final version of the updated SSDF.

(iv) Within 120 days of the final update to the SSDF described in subsection (c)(iii) of this section, the Director of OMB shall incorporate select practices for the secure development and delivery of software contained in NIST's updated SSDF into the requirements of OMB Memorandum M–22–18 (*Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*) or related requirements.

(v) Within 30 days of the issuance of OMB's updated requirements described in subsection (c)(iv) of this section, the Director of CISA shall prepare any revisions to CISA's common form for Secure Software Development Attestation to conform to OMB's requirements and shall initiate any process required to obtain clearance of the revised form under the Paperwork Reduction Act, 44 U.S.C. 3501 *et seq.*

(d) As agencies have improved their cyber defenses, adversaries have targeted the weak links in agency supply chains and the products and services upon which the Federal Government relies. Agencies need to integrate cybersecurity supply chain risk management programs into enterprise-wide risk management activities. Within 90 days of the date of this order, the Director of OMB, in coordination with the Secretary of Commerce, acting through the Director of NIST, the Administrator of General Services, and the Federal Acquisition Security Council (FASC), shall take steps to require, as the Director deems appropriate, that agencies comply with the guidance in NIST Special Publication 800–161 (*Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* (SP 800–161 Revision 1)). OMB shall require agencies to provide annual updates to OMB as they complete implementation. Consistent with SP 800–161 Revision 1, OMB's requirements shall address the integration of cybersecurity into the acquisition lifecycle through acquisition planning, source selection, responsibility determination, security compliance evaluation, contract administration, and performance evaluation.

(e) Open source software plays a critical role in Federal information systems. To help the Federal Government continue to reap the innovation and cost benefits of open source software and contribute to the cybersecurity of the open source software ecosystem, agencies must better manage their use of open source software. Within 120 days of the date of this order, the Secretary of Homeland Security, acting through the Director of CISA, and the Director of OMB, in consultation with the Administrator of General Services and the heads of other agencies as appropriate, shall jointly issue recommendations to agencies on the use of security assessments and patching of open source software and best practices for contributing to open source software projects.

Sec. 3. Improving the Cybersecurity of Federal Systems. (a) The Federal Government must adopt proven security practices from industry—to include

in identity and access management—in order to improve visibility of security threats across networks and strengthen cloud security.

(b) To prioritize investments in the innovative identity technologies and processes of the future and phishing-resistant authentication options, FCEB agencies shall begin using, in pilot deployments or in larger deployments as appropriate, commercial phishing-resistant standards such as WebAuthn, building on the deployments that OMB and CISA have developed and established since the issuance of Executive Order 14028. These pilot deployments shall be used to inform future directions for Federal identity, credentialing, and access management strategies.

(c) The Federal Government must maintain the ability to rapidly and effectively identify threats across the Federal enterprise. In Executive Order 14028, I directed the Secretary of Defense and the Secretary of Homeland Security to establish procedures to immediately share threat information to strengthen the collective defense of Department of Defense and civilian networks. To enable identification of threat activity, CISA's capability to hunt for and identify threats across FCEB agencies under 44 U.S.C. 3553(b)(7) must be strengthened.

(i) The Secretary of Homeland Security, acting through the Director of CISA, in coordination with the Federal Chief Information Officer (CIO) Council and Federal Chief Information Security Officer (CISO) Council, shall develop the technical capability to gain timely access to required data from FCEB agency endpoint detection and response (EDR) solutions and from FCEB agency security operation centers to enable:

(A) timely hunting and identification of novel cyber threats and vulnerabilities across the Federal civilian enterprise;

(B) identification of coordinated cyber campaigns that simultaneously target multiple agencies and move laterally across the Federal enterprise; and

(C) coordination of Government-wide efforts on information security policies and practices, including compilation and analysis of information about incidents that threaten information security.

(ii) Within 180 days of the date of this order, the Secretary of Homeland Security, acting through the Director of CISA, in coordination with the Federal CIO and CISO Councils, shall develop and release a concept of operations that enables CISA to gain timely access to required data to achieve the objectives described in subsection (c)(i) of this section. The Director of OMB shall oversee the development of this concept of operations to account for agency perspectives and the objectives outlined in this section and shall approve the final concept of operations. This concept of operations shall include:

(A) requirements for FCEB agencies to provide CISA with data of sufficient completeness and on the timeline required to enable CISA to achieve the objectives described in subsection (c)(i) of this section;

(B) requirements for CISA to provide FCEB agencies with advanced notification when CISA directly accesses agency EDR solutions to obtain required telemetry;

(C) specific use cases for which agencies may provide telemetry data subject to the requirements in subsection (c)(ii)(A) of this section as opposed to direct access to EDR solutions by CISA;

(D) high-level technical and policy control requirements to govern CISA access to agency EDR solutions that conform with widely accepted cybersecurity principles, including role-based access controls, "least privilege," and separation of duties;

(E) specific protections for highly sensitive agency data that is subject to statutory, regulatory, or judicial restrictions to protect confidentiality or integrity; and

(F) an appendix to the concept of operations that identifies and addresses certain types of specific use cases under subsection (c)(ii)(C) of this section that apply to the Department of Justice, including certain categories of information described in subsections (c)(vi) and (c)(vii) of this section, and requires the Department of Justice's concurrence on the terms of the appendix prior to implementation of the concept of operations on the Department of Justice's or its subcomponents' networks.

(iii) In undertaking the activities described in subsection (c) of this section, the Secretary of Homeland Security, acting through the Director of CISA, shall only make a change to an agency network, system, or data when such change is required for threat hunting by CISA, including access to the EDR tools described in subsection (c)(ii) of this section, or in furtherance of its authority to conduct threat hunting as authorized under 44 U.S.C. 3553(b)(7), unless otherwise authorized by the agency.

(iv) Within 30 days of the release of the concept of operations described in subsection (c)(ii) of this section, the Secretary of Homeland Security, acting through the Director of CISA, shall establish working groups, open to all agencies, to develop and release specific technical controls that achieve the objectives set forth in subsection (c)(ii) of this section and to work with EDR solution providers to implement those controls in FCEB agency deployments of EDR solutions. The Secretary of Homeland Security, acting through the Director of CISA, shall, at a minimum, establish a working group for each EDR solution authorized by CISA for use in the CISA Continuous Diagnostic and Mitigation Program. Each working group shall be open to all agencies and include at least one representative from an FCEB agency employing the designated EDR solution.

(v) Within 180 days of the release of the technical controls described in subsection (c)(iv) of this section, the heads of FCEB agencies shall enroll endpoints using an EDR solution covered by those controls in the CISA Persistent Access Capability program.

(vi) Within 90 days of the date of this order, and periodically thereafter as needed, the heads of FCEB agencies shall provide to CISA a list of systems, endpoints, and data sets that require additional controls or periods of non-disruption to ensure that CISA's threat-hunting activities do not disrupt mission-critical operations, along with an explanation of those operations.

(vii) In cases in which agency data is subject to statutory, regulatory, or judicial access restrictions, the Director of CISA shall comply with agency processes and procedures required to access such data or work with the agency to develop an appropriate administrative accommodation consistent with any such restrictions so that the data is not subject to unauthorized access or use.

(viii) Nothing in this order requires an agency to provide access to information that is protected from non-disclosure by court order or otherwise required to be kept confidential in connection with a judicial proceeding.

(d) The security of Federal information systems relies on the security of the Government's cloud services. Within 90 days of the date of this order, the Administrator of General Services, acting through the Director of the Federal Risk and Authorization Management Program (FedRAMP), in coordination with the Secretary of Commerce, acting through the Director of NIST, and the Secretary of Homeland Security, acting through the Director of CISA, shall develop FedRAMP policies and practices to incentivize or require cloud service providers in the FedRAMP Marketplace to produce baselines with specifications and recommendations for agency configuration of agency cloud-based systems in order to secure Federal data based on agency requirements.

(e) As cybersecurity threats to space systems increase, these systems and their supporting digital infrastructure must be designed to adapt to evolving cybersecurity threats and operate in contested environments. In light of

the pivotal role space systems play in global critical infrastructure and communications resilience, and to further protect space systems and the supporting digital infrastructure vital to our national security, including our economic security, agencies shall take steps to continually verify that Federal space systems have the requisite cybersecurity capabilities through actions including continuous assessments, testing, exercises, and modeling and simulation.

(i) Within 180 days of the date of this order, the Secretary of the Interior, acting through the Director of the United States Geological Survey; the Secretary of Commerce, acting through the Under Secretary of Commerce for Oceans and Atmosphere and the Administrator of the National Oceanic and Atmospheric Administration; and the Administrator of the National Aeronautics and Space Administration shall each review the civil space contract requirements in the FAR and recommend to the FAR Council and other appropriate agencies updates to civil space cybersecurity requirements and relevant contract language. The recommended cybersecurity requirements and contract language shall use a risk-based, tiered approach for all new civil space systems. Such requirements shall be designed to apply at minimum to the civil space systems' on-orbit segments and link segments. The requirements shall address the following elements for the highest-risk tier and, as appropriate, other tiers:

(A) protection of command and control of the civil space system, including backup or failover systems, by:

- (1) encrypting commands to protect the confidentiality of communications;
- (2) ensuring commands are not modified in transit;
- (3) ensuring an authorized party is the source of commands; and
- (4) rejecting unauthorized command and control attempts;

(B) establishment of methods to detect, report, and recover from anomalous network or system activity; and

(C) use of secure software and hardware development practices, consistent with the NIST SSDF or any successor documents.

(ii) Within 180 days of receiving the recommended contract language described in subsection (e)(i) of this section, the FAR Council shall review the proposal and, as appropriate and consistent with applicable law, the agency members of the FAR Council shall jointly take steps to amend the FAR.

(iii) Within 120 days of the date of this order, the National Cyber Director shall submit to OMB a study of space ground systems owned, managed, or operated by FCEB agencies. This study shall include:

(A) an inventory of space ground systems;

(B) whether each space ground system is classified as a major information system under 44 U.S.C. 3505(c), labeled "Inventory of major information systems"; and

(C) recommendations to improve the cyber defenses and oversight of such space ground systems.

(iv) Within 90 days of the submission of the study described in subsection (e)(iii) of this section, the Director of OMB shall take appropriate steps to help ensure that space ground systems owned, managed, or operated by FCEB agencies comply with relevant cybersecurity requirements issued by OMB.

Sec. 4. *Securing Federal Communications.* (a) To improve the security of Federal Government communications against adversarial nations and criminals, the Federal Government must implement, to the extent practicable and consistent with mission needs, strong identity authentication and encryption using modern, standardized, and commercially available algorithms and protocols.

(b) The security of internet traffic depends on data being correctly routed and delivered to the intended recipient network. Routing information originated and propagated across the internet, utilizing the Border Gateway Protocol (BGP), is vulnerable to attack and misconfiguration.

(i) Within 90 days of the date of this order, FCEB agencies shall take steps to ensure that all of their assigned internet number resources (internet Protocol (IP) address blocks and Autonomous System Numbers) are covered by a Registration Services Agreement with the American Registry for internet Numbers or another appropriate regional internet registry. Thereafter, FCEB agencies shall annually review and update in their regional internet registry accounts organizational identifiers related to assigned number resources such as organization names, points of contact, and associated email addresses.

(ii) Within 120 days of the date of this order, all FCEB agencies that hold IP address blocks shall create and publish Route Origin Authorizations in the public Resource Public Key Infrastructure repository hosted or delegated by the American Registry for internet Numbers or the appropriate regional internet registry for the IP address blocks they hold.

(iii) Within 120 days of the date of this order, the National Cyber Director, in coordination with the heads of other agencies as appropriate, shall recommend contract language to the FAR Council to require contracted providers of internet services to agencies to adopt and deploy internet routing security technologies, including publishing Route Origin Authorizations and performing Route Origin Validation filtering. The recommended language shall include requirements or exceptions, as appropriate, for agency contracts regarding overseas operations and overseas local service providers. Within 270 days of receiving these recommendations, the FAR Council shall review the recommended contract language and, as appropriate and consistent with applicable law, the agency members of the FAR Council shall jointly take steps to amend the FAR. Pending any such amendments to the FAR, individual agencies are encouraged to include such requirements in future contracts, consistent with applicable law.

(iv) Within 180 days of the date of this order, the Secretary of Commerce, acting through the Director of NIST, shall publish updated guidance to agencies on deployment of current, operationally viable BGP security methods for Federal Government networks and service providers. The Secretary of Commerce, acting through the Director of NIST, shall also provide updated guidance on other emerging technologies to improve internet routing security and resilience, such as route leak mitigation and source address validation.

(c) Encrypting Domain Name System (DNS) traffic in transit is a critical step to protecting both the confidentiality of the information being transmitted to, and the integrity of the communication with, the DNS resolver.

(i) Within 90 days of the date of this order, the Secretary of Homeland Security, acting through the Director of CISA, shall publish template contract language requiring that any product that acts as a DNS resolver (whether client or server) for the Federal Government support encrypted DNS and shall recommend that language to the FAR Council. Within 120 days of receiving the recommended language, the FAR Council shall review it, and, as appropriate and consistent with applicable law, the agency members of the FAR Council shall jointly take steps to amend the FAR.

(ii) Within 180 days of the date of this order, FCEB agencies shall enable encrypted DNS protocols wherever their existing clients and servers support those protocols. FCEB agencies shall also enable such protocols within 180 days of any additional clients and servers supporting such protocols.

(d) The Federal Government must encrypt email messages in transport and, where practical, use end-to-end encryption in order to protect messages from compromise.

(i) Within 120 days of the date of this order, each FCEB agency shall technically enforce encrypted and authenticated transport for all connections between the agency's email clients and their associated email servers.

(ii) Within 180 days of the date of this order, the Director of OMB shall establish a requirement for expanded use of authenticated transport-layer encryption between email servers used by FCEB agencies to send and receive email.

(iii) Within 90 days of the establishment of the requirement described in subsection (d)(ii) of this section, the Secretary of Homeland Security, acting through the Director of CISA, shall take appropriate steps to assist agencies in meeting that requirement, including by issuing implementing directives, as well as technical guidance to address any identified capability gaps.

(e) Modern communications such as voice and video conferencing and instant messaging are usually encrypted at the link level but often are not encrypted end-to-end. Within 180 days of the date of this order, to advance the security of internet-based voice and video conferencing and instant messaging, the Director of OMB, in coordination with the Secretary of Homeland Security, acting through the Director of CISA; the Secretary of Defense, acting through the Director of the National Security Agency (NSA); the Secretary of Commerce, acting through the Director of NIST; the Archivist of the United States, acting through the Chief Records Officer for the United States Government; and the Administrator of General Services shall take appropriate steps to require agencies to:

(i) enable transport encryption by default; and

(ii) where technically supported, use end-to-end encryption by default while maintaining logging and archival capabilities that allow agencies to fulfill records management and accountability requirements.

(f) Alongside their benefits, quantum computers pose significant risk to the national security, including the economic security, of the United States. Most notably, a quantum computer of sufficient size and sophistication—also known as a cryptanalytically relevant quantum computer (CRQC)—will be capable of breaking much of the public-key cryptography used on digital systems across the United States and around the world. In National Security Memorandum 10 of May 4, 2022 (Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems), I directed the Federal Government to prepare for a transition to cryptographic algorithms that would not be vulnerable to a CRQC.

(i) Within 180 days of the date of this order, the Secretary of Homeland Security, acting through the Director of CISA, shall release and thereafter regularly update a list of product categories in which products that support post-quantum cryptography (PQC) are widely available.

(ii) Within 90 days of a product category being placed on the list described in subsection (f)(i) of this section, agencies shall take steps to include in any solicitations for products in that category a requirement that products support PQC.

(iii) Agencies shall implement PQC key establishment or hybrid key establishment including a PQC algorithm as soon as practicable upon support being provided by network security products and services already deployed in their network architectures.

(iv) Within 90 days of the date of this order, the Secretary of State and the Secretary of Commerce, acting through the Director of NIST and the Under Secretary for International Trade, shall identify and engage foreign governments and industry groups in key countries to encourage their transition to PQC algorithms standardized by NIST.

(v) Within 180 days of the date of this order, to prepare for transition to PQC, the Secretary of Defense with respect to National Security Systems (NSS), and the Director of OMB with respect to non-NSS, shall each

issue requirements for agencies to support, as soon as practicable, but not later than January 2, 2030, Transport Layer Security protocol version 1.3 or a successor version.

(g) The Federal Government should take advantage of commercial security technologies and architectures, such as hardware security modules, trusted execution environments, and other isolation technologies, to protect and audit access to cryptographic keys with extended lifecycles.

(i) Within 270 days of the date of this order, the Secretary of Commerce, acting through the Director of NIST, in consultation with the Secretary of Homeland Security, acting through the Director of CISA, and the Administrator of General Services shall develop guidelines for the secure management of access tokens and cryptographic keys used by cloud service providers.

(ii) Within 60 days of the publication of the guidelines described in subsection (g)(i) of this section, the Administrator of General Services, acting through the FedRAMP Director, in consultation with the Secretary of Commerce, acting through the Director of NIST, and the Secretary of Homeland Security, acting through the Director of CISA, shall develop updated FedRAMP requirements, incorporating the guidelines described in subsection (g)(i) of this section, as appropriate and consistent with guidance issued by the Director of OMB, concerning cryptographic key management security practices.

(iii) Within 60 days of the publication of the guidelines described in subsection (g)(i) of this section, the Director of OMB, in consultation with the Secretary of Commerce, acting through the Director of NIST; the Secretary of Homeland Security, acting through the Director of CISA; and the Administrator of General Services shall take appropriate steps to require FCEB agencies to follow best practices concerning the protection and management of hardware security modules, trusted execution environments, or other isolation technologies for access tokens and cryptographic keys used by cloud service providers in the provision of services to agencies.

Sec. 5. Solutions to Combat Cybercrime and Fraud. (a) The use of stolen and synthetic identities by criminal syndicates to systemically defraud public benefits programs costs taxpayers and wastes Federal Government funds. To help address these crimes it is the policy of the executive branch to strongly encourage the acceptance of digital identity documents to access public benefits programs that require identity verification, so long as it is done in a manner that preserves broad program access for vulnerable populations and supports the principles of privacy, data minimization, and interoperability.

(i) Within 90 days of the date of this order, agencies with grantmaking authority are encouraged to consider, in coordination with OMB and the National Security Council staff, whether Federal grant funding is available to assist States in developing and issuing mobile driver's licenses that achieve the policies and principles described in this section.

(ii) Within 270 days of the date of this order, the Secretary of Commerce, acting through the Director of NIST, shall issue practical implementation guidance, in collaboration with relevant agencies and other stakeholders through the National Cybersecurity Center of Excellence, to support remote digital identity verification using digital identity documents that will help issuers and verifiers of digital identity documents advance the policies and principles described in this section.

(iii) Agencies should consider accepting digital identity documents as digital identity verification evidence to access public benefits programs, but only if the use of these documents is consistent with the policies and principles described in this section.

(iv) Agencies should, consistent with applicable law, seek to ensure that digital identity documents accepted as digital identity verification evidence to access public benefits programs:

(A) are interoperable with relevant standards and trust frameworks, so that the public can use any standards-compliant hardware or software containing an official Government-issued digital identity document, regardless of manufacturer or developer;

(B) do not enable authorities that issue digital identity documents, device manufacturers, or any other third party to surveil or track presentation of the digital identity document, including user device location at the time of presentation; and

(C) support user privacy and data minimization by ensuring only the minimum information required for a transaction—often a “yes” or “no” response to a question, such as whether an individual is older than a specific age—is requested from the holder of the digital identity document.

(b) The use of “Yes/No” validation services, also referred to as attribute validation services, can enable more privacy-preserving means to reduce identity fraud. These services allow programs to confirm, via a privacy-preserving “yes” or “no” response, that applicant-provided identity information is consistent with information already contained in official records, without needing to share the contents of those official records. To support the use of such services, the Commissioner of Social Security, and the head of any other agency designated by the Director of OMB, shall, as appropriate and consistent with applicable law, consider taking steps to develop or modify services—including through, as appropriate, the initiation of a proposed rulemaking or the publication of a notice of a new or significantly modified routine use of records—related to Government-operated identity verification systems and public benefits programs, with consideration given to having such systems and programs submit applicant-provided identity information to the agency providing the service and receive a “yes” or “no” response as to whether the applicant-provided identity information is consistent with the information on file with the agency providing the service. In doing so, the heads of these agencies shall specifically consider seeking to ensure, consistent with applicable law, that:

(i) any applicant-provided identity information submitted to the services and any “yes” or “no” response provided by the services are used only to assist with identity verification, program administration, anti-fraud operations, or investigation and prosecution of fraud related to the public benefits program for which the identity information was submitted;

(ii) the services are made available, to the maximum extent permissible and as appropriate, to public benefits programs; Government-operated identity verification systems, including shared-service providers; payment integrity programs; and United States-regulated financial institutions; and

(iii) the agencies, public benefits programs, or institutions using the services provide reimbursement to appropriately cover costs and support the ongoing maintenance, improvement, and broad accessibility of the services.

(c) The Secretary of the Treasury, in consultation with the Administrator of General Services, shall research, develop, and conduct a pilot program for technology that notifies individuals and entities when their identity information is used to request a payment from a public benefits program, gives individuals and entities the option to stop potentially fraudulent transactions before they occur, and reports fraudulent transactions to law enforcement entities.

Sec. 6. *Promoting Security with and in Artificial Intelligence.* Artificial intelligence (AI) has the potential to transform cyber defense by rapidly identifying new vulnerabilities, increasing the scale of threat detection techniques, and automating cyber defense. The Federal Government must accelerate the development and deployment of AI, explore ways to improve the cybersecurity of critical infrastructure using AI, and accelerate research at the intersection of AI and cybersecurity.

(a) Within 180 days of the date of the completion of the Defense Advanced Research Projects Agency’s 2025 Artificial Intelligence Cyber Challenge, the Secretary of Energy, in coordination with the Secretary of Defense, acting

(C) address how agencies should identify, assess, respond to, and mitigate risks to mission essential functions presented by concentration of IT vendors and services.

(ii) The Secretary of Commerce, acting through the Director of NIST; the Secretary of Homeland Security, acting through the Director of CISA; and the Director of OMB shall establish a pilot program of a rules-as-code approach for machine-readable versions of policy and guidance that OMB, NIST, and CISA publish and manage regarding cybersecurity.

(b) Managing cybersecurity risks is now a part of everyday industry practice and should be expected for all types of businesses. Minimum cybersecurity requirements can make it costlier and harder for threat actors to compromise networks. Within 240 days of the date of this order, the Secretary of Commerce, acting through the Director of NIST, shall evaluate common cybersecurity practices and security control outcomes that are commonly used or recommended across industry sectors, international standards bodies, and other risk management programs, and based on that evaluation issue guidance identifying minimum cybersecurity practices. In developing this guidance, the Secretary of Commerce, acting through the Director of NIST, shall solicit input from the Federal Government, the private sector, academia, and other appropriate actors.

(c) Agencies face multiple cybersecurity risks when purchasing products and services. While agencies have already made significant advances to improve their supply chain risk management, additional actions are needed to keep pace with the evolving threat landscape. Within 180 days of the issuance of the guidance described in subsection (b) of this section, the FAR Council shall review the guidance and, as appropriate and consistent with applicable law, the agency members of the FAR Council shall jointly take steps to amend the FAR to:

(i) require that contractors with the Federal Government follow applicable minimum cybersecurity practices identified in NIST's guidance pursuant to subsection (b) of this section with respect to work performed under agency contracts or when developing, maintaining, or supporting IT services or products that are provided to the Federal Government; and

(ii) adopt requirements for agencies to, by January 4, 2027, require vendors to the Federal Government of consumer internet-of-things products, as defined by 47 CFR 8.203(b), to carry United States Cyber Trust Mark labeling for those products.

Sec. 8. National Security Systems and Debilitating Impact Systems. (a) Except as specifically provided for in section 4(f)(v) of this order, sections 1 through 7 of this order shall not apply to Federal information systems that are NSS or are otherwise identified by the Department of Defense or the Intelligence Community as debilitating impact systems.

(b) Within 90 days of the date of this order, to help ensure that NSS and debilitating impact systems are protected with the most advanced security measures, the Secretary of Defense, acting through the Director of NSA as the National Manager for National Security Systems (National Manager), in coordination with the Director of National Intelligence and the Committee on National Security Systems (CNSS), and in consultation with the Director of OMB and the Assistant to the President for National Security Affairs (APNSA), shall develop requirements for NSS and debilitating impact systems that are consistent with the requirements set forth in this order, as appropriate and consistent with applicable law. The Secretary of Defense may grant exceptions to such requirements in circumstances necessitated by unique mission needs. Such requirements shall be incorporated into a proposed National Security Memorandum, to be submitted to the President through the APNSA.

(c) To help protect space NSS with cybersecurity measures that keep pace with emerging threats, within 210 days of the date of this order, the CNSS shall review and update, as appropriate, relevant policies and guidance regarding space system cybersecurity. In addition to appropriate

Presidential Documents

Executive Order 14136 of January 3, 2025

Providing an Order of Succession Within the Department of Justice

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the Federal Vacancies Reform Act of 1998, as amended, 5 U.S.C. 3345 *et seq.* (the “Act”), it is hereby ordered that:

Section 1. Order of Succession. Subject to the provisions of section 2 of this order, and to the limitations set forth in the Act, the following officials of the Department of Justice, in the order listed, shall act as and perform the functions and duties of the office of Attorney General during any period in which the Attorney General, the Deputy Attorney General, the Associate Attorney General, and any officers designated by the Attorney General pursuant to 28 U.S.C. 508 to act as Attorney General have died, resigned, or otherwise become unable to perform the functions and duties of the office of Attorney General, until such time as at least one of the officers mentioned above is able to perform the functions and duties of that office:

- (a) United States Attorney for the Southern District of New York;
- (b) United States Attorney for the District of Arizona;
- (c) United States Attorney for the Northern District of Illinois; and
- (d) United States Attorney for the District of Hawaii.

Sec. 2. Exceptions. (a) No individual who is serving in an office listed in section 1(a)–(d) of this order in an acting capacity shall, by virtue of so serving, act as Attorney General pursuant to this order.

(b) No individual who is serving in an office listed in section 1(a)–(d) of this order shall act as Attorney General unless that individual is otherwise eligible to so serve under the Act.

(c) Notwithstanding the provisions of this order, the President retains discretion, to the extent permitted by law, to depart from this order in designating an acting Attorney General.

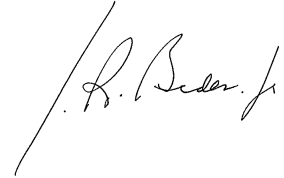
Sec. 3. Revocation. Executive Order 13787 of March 31, 2017 (Providing an Order of Succession Within the Department of Justice), is hereby revoked.

Sec. 4. 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.



THE WHITE HOUSE,
January 3, 2025.

through the Director of the Defense Advanced Research Projects Agency, and the Secretary of Homeland Security, shall launch a pilot program, involving collaboration with private sector critical infrastructure entities as appropriate and consistent with applicable law, on the use of AI to enhance cyber defense of critical infrastructure in the energy sector, and conduct an assessment of the pilot program upon its completion. This pilot program, and accompanying assessment, may include vulnerability detection, automatic patch management, and the identification and categorization of anomalous and malicious activity across information technology (IT) or operational technology systems.

(b) Within 270 days of the date of this order, the Secretary of Defense shall establish a program to use advanced AI models for cyber defense.

(c) Within 150 days of the date of this order, the Secretary of Commerce, acting through the Director of NIST; the Secretary of Energy; the Secretary of Homeland Security, acting through the Under Secretary for Science and Technology; and the Director of the National Science Foundation (NSF) shall each prioritize funding for their respective programs that encourage the development of large-scale, labeled datasets needed to make progress on cyber defense research, and ensure that existing datasets for cyber defense research have been made accessible to the broader academic research community (either securely or publicly) to the maximum extent feasible, in consideration of business confidentiality and national security.

(d) Within 150 days of the date of this order, the Secretary of Commerce, acting through the Director of NIST; the Secretary of Energy; the Secretary of Homeland Security, acting through the Under Secretary for Science and Technology; and the Director of the NSF shall prioritize research on the following topics:

- (i) human-AI interaction methods to assist defensive cyber analysis;
- (ii) security of AI coding assistance, including security of AI-generated code;
- (iii) methods for designing secure AI systems; and
- (iv) methods for prevention, response, remediation, and recovery of cyber incidents involving AI systems.

(e) Within 150 days of the date of this order, the Secretary of Defense, the Secretary of Homeland Security, and the Director of National Intelligence, in coordination with the Director of OMB, shall incorporate management of AI software vulnerabilities and compromises into their respective agencies' existing processes and interagency coordination mechanisms for vulnerability management, including through incident tracking, response, and reporting, and by sharing indicators of compromise for AI systems.

Sec. 7. *Aligning Policy to Practice.* (a) IT infrastructure and networks that support agencies' critical missions need to be modernized. Agencies' policies must align investments and priorities to improve network visibility and security controls to reduce cyber risks.

(i) Within 3 years of the date of this order, the Director of OMB shall issue guidance, including any necessary revision to OMB Circular A-130, to address critical risks and adapt modern practices and architectures across Federal information systems and networks. This guidance shall, at a minimum:

(A) outline expectations for agency cybersecurity information sharing and exchange, enterprise visibility, and accountability for enterprise-wide cybersecurity programs by agency CISOs;

(B) revise OMB Circular A-130 to be less technically prescriptive in key areas, where appropriate, to more clearly promote the adoption of evolving cybersecurity best practices across Federal systems, and to include migration to zero trust architectures and implementation of critical elements such as EDR capabilities, encryption, network segmentation, and phishing-resistant multi-factor authentication; and

updates, the CNSS shall identify and address appropriate requirements to implement cyber defenses on Federal Government-procured space NSS in the areas of intrusion detection, use of hardware roots of trust for secure booting, and development and deployment of security patches.

(d) To enhance the effective governance and oversight of Federal information systems, within 90 days of the date of this order, the Director of OMB shall issue guidance as appropriate requiring agencies to inventory all major information systems and provide the inventory to CISA, the Department of Defense, or the National Manager, as applicable, which shall each maintain a registry of agency inventories within their purview. CISA, the Department of Defense CIO, and the National Manager will share their inventories as appropriate to identify gaps or overlaps in oversight coverage. This guidance shall not apply to elements of the Intelligence Community.

(e) Nothing in this order alters the authorities and responsibilities granted in law or policy to the Director of National Intelligence, the Secretary of Defense, and the National Manager over applicable systems pursuant to the National Security Act of 1947 (Public Law 80–253), the Federal Information Security Modernization Act of 2014 (Public Law 113–283), National Security Directive 42 of July 5, 1990 (National Policy for the Security of National Security Telecommunications and Information Systems), or National Security Memorandum 8 of January 19, 2022 (Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems).

Sec. 9. *Additional Steps to Combat Significant Malicious Cyber-Enabled Activities.* Because I find that additional steps must be taken to deal with the national emergency with respect to significant malicious cyber-enabled activities declared in Executive Order 13694 of April 1, 2015 (Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities), as amended by Executive Order 13757 of December 28, 2016 (Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities), and further amended by Executive Order 13984 of January 19, 2021 (Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities), to protect against the growing and evolving threat of malicious cyber-enabled activities against the United States and United States allies and partners, including the increasing threats by foreign actors of unauthorized access to critical infrastructure, ransomware, and cyber-enabled intrusions and sanctions evasion, I hereby order that section 1(a) of Executive Order 13694 is further amended to read as follows:

“**Section 1.** (a) All property and interests in property that are in the United States, that hereafter come within the United States, or that are or hereafter come within the possession or control of any United States person of the following persons are blocked and may not be transferred, paid, exported, withdrawn, or otherwise dealt in:

(i) the persons listed in the Annex to this order;

(ii) any person determined by the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, to be responsible for or complicit in, or to have engaged in, directly or indirectly, cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States that are reasonably likely to result in, or have materially contributed to, a threat to the national security, foreign policy, or economic health or financial stability of the United States, and that have the purpose of or involve:

(A) harming, or otherwise compromising the provision of services by, a computer or network of computers that support one or more entities in a critical infrastructure sector;

(B) compromising the provision of services by one or more entities in a critical infrastructure sector;

(C) causing a disruption to the availability of a computer or network of computers or compromising the integrity of the information stored on a computer or network of computers;

(D) causing a misappropriation of funds or economic resources, intellectual property, proprietary or business confidential information, personal identifiers, or financial information for commercial or competitive advantage or private financial gain;

(E) tampering with, altering, or causing a misappropriation of information with the purpose of or that involves interfering with or undermining election processes or institutions; or

(F) engaging in a ransomware attack, such as extortion through malicious use of code, encryption, or other activity to affect the confidentiality, integrity, or availability of data or a computer or network of computers, against a United States person, the United States, a United States ally or partner or a citizen, national, or entity organized under the laws thereof; or

(iii) any person determined by the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State:

(A) to be responsible for or complicit in, or to have engaged in, directly or indirectly, the receipt or use for commercial or competitive advantage or private financial gain, or by a commercial entity, outside the United States of funds or economic resources, intellectual property, proprietary or business confidential information, personal identifiers, or financial information misappropriated through cyber-enabled means, knowing they have been misappropriated, where the misappropriation of such funds or economic resources, intellectual property, proprietary or business confidential information, personal identifiers, or financial information is reasonably likely to result in, or has materially contributed to, a threat to the national security, foreign policy, or economic health or financial stability of the United States;

(B) to be responsible for or complicit in, or to have engaged in, directly or indirectly, activities related to gaining or attempting to gain unauthorized access to a computer or network of computers of a United States person, the United States, a United States ally or partner or a citizen, national, or entity organized under the laws thereof, where such efforts originate from or are directed by persons located, in whole or substantial part, outside the United States and are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States;

(C) to have materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, any activity described in subsections (a)(ii) or (a)(iii)(A) or (B) of this section or any person whose property and interests in property are blocked pursuant to this order;

(D) to be owned or controlled by, or to have acted or purported to act for or on behalf of, directly or indirectly, any person whose property and interests in property are blocked pursuant to this order or that has engaged in any activity described in subsections (a)(ii) or (a)(iii)(A)–(C) of this section;

(E) to have attempted to engage in any of the activities described in subsections (a)(ii) and (a)(iii)(A)–(D) of this section; or

(F) to be or have been a leader, official, senior executive officer, or member of the board of directors of any person whose property and interests in property are blocked pursuant to this order or that has engaged in any activity described in subsections (a)(ii) or (a)(iii)(A) – (E) of this section.”

Sec. 10. Definitions. For purposes of this order:

(a) The term “agency” has the meaning ascribed to it under 44 U.S.C. 3502(1), except for the independent regulatory agencies described in 44 U.S.C. 3502(5).

(b) The term “artifact” means a record or data that is generated manually or by automated means and may be used to demonstrate compliance with defined practices, including for secure software development.

(c) The term “artificial intelligence” or “AI” has the meaning set forth in 15 U.S.C. 9401(3).

(d) The term “AI system” means any data system, software, hardware, application, tool, or utility that operates in whole or in part using AI.

(e) The term “authentication” means the process of determining the validity of one or more authenticators, such as a password, used to claim a digital identity.

(f) The term “Border Gateway Protocol” or “BGP” means the control protocol used to distribute and compute paths between the tens of thousands of autonomous networks that constitute the internet.

(g) The term “consumer internet-of-Things products” means internet-of-Things products intended primarily for consumer use, rather than enterprise or industrial use. Consumer internet-of-Things products do not include medical devices regulated by the United States Food and Drug Administration or motor vehicles and motor vehicle equipment regulated by the National Highway Traffic Safety Administration.

(h) The term “cyber incident” has the meaning given to the term “incident” under 44 U.S.C. 3552(b)(2).

(i) The term “debilitating impact systems” means systems as described by 44 U.S.C. 3553(e)(2) and 3553(e)(3) for Department of Defense and Intelligence Community purposes, respectively.

(j) The term “digital identity document” means an electronic, reusable, cryptographically verifiable identity credential issued by a Government source, such as a State-issued mobile driver’s license or an electronic passport.

(k) The term “digital identity verification” means identity verification that a user performs online.

(l) The term “endpoint” means any device that can be connected to a computer network creating an entry or exit point for data communications. Examples of endpoints include desktop and laptop computers, smartphones, tablets, servers, workstations, virtual machines, and consumer internet-of-Things products.

(m) The term “endpoint detection and response” means cybersecurity tools and capabilities that combine real-time continuous monitoring and collection of endpoint data (for example, networked computing device such as workstations, mobile phones, servers) with rules-based automated response and analysis capabilities.

(n) The term “Federal Civilian Executive Branch agencies” or “FCEB agencies” includes all agencies except for the agencies and other components in the Department of Defense and agencies in the Intelligence Community.

(o) The term “Federal information system” means an information system used or operated by an agency, a contractor of an agency, or another organization on behalf of an agency.

(p) The term “Government-operated identity verification system” means a system owned and operated by a Federal, State, local, Tribal, or territorial Government entity that performs identity verification, including single-agency systems and shared services that provide service to multiple agencies.

(q) The term “hardware root of trust” means an inherently trusted combination of hardware and firmware that helps to maintain the integrity of information.

(r) The term “hybrid key establishment” means a key establishment scheme that is a combination of two or more components that are themselves cryptographic key-establishment schemes.

(s) The term “identity verification” means the process of collecting identity information or evidence, validating its legitimacy, and confirming that it is associated with the real person providing it.

(t) The term “Intelligence Community” has the meaning given to it under 50 U.S.C. 3003(4).

(u) The term “key establishment” means the process by which a cryptographic key is securely shared between two or more entities.

(v) The term “least privilege” means the principle that a security architecture is designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

(w) The term “machine-readable” means that the product output is in a structured format that can be consumed by another program using consistent processing logic.

(x) The term “national security systems” or “NSS” has the meaning given to it under 44 U.S.C. 3552(b)(6).

(y) The term “patch” means a software component that, when installed, directly modifies files or device settings related to a different software component without changing the version number or release details for the related software component.

(z) The term “rules-as-code approach” means a coded version of rules (for example, those contained in legislation, regulation, or policy) that can be understood and used by a computer.

(aa) The term “secure booting” means a security feature that prevents malicious software from running when a computer system starts up. The security feature performs a series of checks during the boot sequence that helps ensure only trusted software is loaded.

(bb) The term “security control outcome” means the results of the performance or non-performance of safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information.

(cc) The term “zero trust architecture” has the meaning given to it in Executive Order 14028.

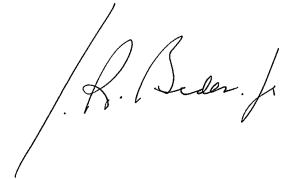
Sec. 11. General Provisions. (a) Nothing in this order shall be construed to impair or otherwise affect:

(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 in a manner 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.



THE WHITE HOUSE,
January 16, 2025.

Presidential Documents

Executive Order 14140 of January 8, 2025

Taking Additional Steps With Respect to the Situation in the Western Balkans

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the International Emergency Economic Powers Act (50 U.S.C. 1701 *et seq.*) (IEEPA), the National Emergencies Act (50 U.S.C. 1601 *et seq.*) (NEA), section 212(f) of the Immigration and Nationality Act of 1952 (8 U.S.C. 1182(f)), and section 301 of title 3, United States Code,

I, JOSEPH R. BIDEN JR., President of the United States of America, in view of events in the Western Balkans, including continued attempts by individuals to challenge the sovereignty and territorial integrity of Western Balkans nations, to undermine post-war agreements and institutions, to engage in significant corruption that erodes the rule of law and trust in democratic governance, and to evade United States Government sanctions, and in order to take additional steps with respect to the national emergency declared in Executive Order 13219 of June 26, 2001 (Blocking Property of Persons Who Threaten International Stabilization Efforts in the Western Balkans), as amended by Executive Order 13304 of May 28, 2003 (Termination of Emergencies With Respect to Yugoslavia and Modification of Executive Order 13219 of June 26, 2001), and expanded in scope by Executive Order 14033 of June 8, 2021 (Blocking Property and Suspending Entry Into the United States of Certain Persons Contributing to the Destabilizing Situation in the Western Balkans), hereby order:

Section 1. Amendments to Executive Order 14033. Executive Order 14033 is hereby amended by striking section 1 and inserting, in lieu thereof, the following:

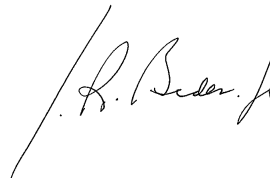
“**Section 1.** (a) All property and interests in property that are in the United States, that hereafter come within the United States, or that are or hereafter come within the possession or control of any United States person of the following persons are blocked and may not be transferred, paid, exported, withdrawn, or otherwise dealt in: any person determined by the Secretary of the Treasury, in consultation with the Secretary of State:

(i) to be responsible for or complicit in, or to have directly or indirectly engaged or attempted to engage in, actions or policies that threaten the peace, security, stability, or territorial integrity of any area or state in the Western Balkans;

(ii) to be responsible for or complicit in, including by involvement in developing, or to have directly or indirectly engaged or attempted to engage in, actions or policies that undermine democratic processes or institutions in the Western Balkans;

(iii) to be responsible for or complicit in, or to have directly or indirectly engaged or attempted to engage in, a violation of, or an act that has obstructed or threatened the implementation of, any regional security, peace, cooperation, or mutual recognition agreement or framework or accountability mechanism, or to pose a significant risk of committing such an act, related to the Western Balkans, including the Prespa Agreement of 2018; the Ohrid Framework Agreement of 2001; United Nations Security Council Resolution 1244; the Dayton Accords; or the Conclusions of the Peace Implementation Conference Council held in London in December

(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.



THE WHITE HOUSE,
January 19, 2025.

1995, including the decisions or conclusions of the High Representative, the Peace Implementation Council, or its Steering Board; or the International Criminal Tribunal for the former Yugoslavia, or, with respect to the former Yugoslavia, the International Residual Mechanism for Criminal Tribunals;

(iv) to be responsible for or complicit in, or to have directly or indirectly engaged or attempted to engage in, serious human rights abuse in the Western Balkans;

(v) to be responsible for or complicit in, or to have directly or indirectly engaged or attempted to engage in, corruption related to the Western Balkans, including corruption by, on behalf of, or otherwise related to a government in the Western Balkans, or a current or former government official at any level of government in the Western Balkans, such as the misappropriation of public assets, expropriation of private assets for personal gain or political purposes, or bribery;

(vi) to be a leader, official, or member of an entity, including a government entity, that has engaged in, or attempted to engage in, any of the activities described in subsections (1)(a)(i)–(v) of this order, or whose property and interests in property are blocked pursuant to this order;

(vii) to have materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, any person whose property and interests in property are blocked pursuant to this order;

(viii) to be owned or controlled by, or to have acted or purported to act for or on behalf of, directly or indirectly, any person whose property and interests in property are blocked pursuant to this order;

(ix) to own or control, directly or indirectly, any person whose property and interests in property are blocked pursuant to this order; or

(x) to be a spouse or adult child of any person whose property and interests in property are blocked pursuant to subsections (1)(a)(i)–(v) of this order.

(b) The prohibitions in subsection (a) of this section apply except to the extent provided by statutes, or in regulations, orders, directives, or licenses that may be issued pursuant to this order, and notwithstanding any contract entered into or any license or permit granted before the date of this order.”

Sec. 2. 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.

Presidential Documents

Title 3—

Executive Order 14145 of January 19, 2025

The President

Helping Left-Behind Communities Make a Comeback

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. *Policy.* Well-designed programs that support local and Tribal leaders in left-behind communities can lead to stronger economic outcomes, strengthen regional assets, and reduce regional inequality. It is the policy of my Administration to take a whole-of-government approach to defining, coordinating, and increasing the accessibility of existing and future programs that help left-behind communities.

Sec. 2. *Definitions.* For purposes of this order:

(a) The term “covered communities” means:

(i) municipalities or other local areas within an economically distressed region;

(ii) communities in Community Disaster Resiliency Zones;

(iii) regions served by any of the following Federal programs: the Energy Communities Interagency Working Group Priority Energy Communities, the Economic Development Administration Regional Technology and Innovation Hubs, the National Science Foundation Regional Innovation Engines, the Department of Housing and Urban Development Distressed Cities and Persistent Poverty Technical Assistance Program, or the Economic Development Administration Recompete Pilot Program; or

(iv) rural communities identified by the Secretary of Agriculture and Administrator of the Environmental Protection Agency.

(b) “Economically distressed region” means a region described by section 301 of the Public Works and Economic Development Act of 1965 (42 U.S.C. 3161), section 29(j) of the Stevenson-Wydler Technology Innovation Act of 1980 (15 U.S.C. 3722b(j)(1)), or 49 U.S.C. 6702(a)(1), or that meets the definition of “persistent poverty county” in section 736 of Division A of Public Law 117–328.

(c) “Implementing agencies” means the Department of the Treasury, the Department of the Interior, the Department of Agriculture, the Department of Commerce, the Department of Labor, the Department of Health and Human Services, the Department of Housing and Urban Development, the Department of Transportation, the Department of Energy, the Department of Homeland Security, the Environmental Protection Agency, and the Small Business Administration.

(d) “Place-based economic development” means policies and programs administered by the Federal Government that target defined regions, including Tribal lands, and use a coordinated approach that represents the interests of community members and community-based organizations in covered communities to:

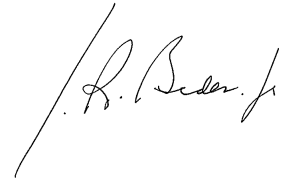
(i) improve physical infrastructure;

(ii) support workforce development to fill locally and regionally demanded well-paying jobs;

(iii) connect regions to new economic opportunities;

(iv) increase the capacity of unions, labor organizations, community organizations, and the general public to negotiate legally binding agreements

(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 persons.



THE WHITE HOUSE,
January 8, 2025.

Presidential Documents

Executive Order 14146 of January 19, 2025

Partial Revocation of Executive Order 13961

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

Section 1. *Revocation.* Sections 1, 3, 4, 5, and 7 of Executive Order 13961 of December 7, 2020 (Governance and Integration of Federal Mission Resilience), are hereby revoked. Sections 2, 6, and 8 of Executive Order 13961 are renumbered as Sections 1, 2, and 3, respectively. Section 1 of Executive Order 13961, as renumbered, is amended by striking the clause “To achieve this policy, in conjunction” and inserting in its place the words “In conjunction”. Section 2(b) of Executive Order 13961, as renumbered, is amended by striking the clause “the Executive Committee established in section 3 of this order” and inserting in its place the words “the Restricted Principals Committee described in section 3 of the National Security Memorandum of January 19, 2025 (National Continuity Policy)”.

Sec. 2. *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.

Presidential Documents

Executive Order 14135 of January 3, 2025

Providing an Order of Succession Within the Department of Homeland Security

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the Federal Vacancies Reform Act of 1998, as amended, 5 U.S.C. 3345 *et seq.* (the “Act”), it is hereby ordered that:

Section 1. Order of Succession. Subject to the provisions of section 2 of this order, and to the limitations set forth in the Act, the following officials of the Department of Homeland Security, in the order listed, shall act as and perform the functions and duties of the office of Secretary of Homeland Security (Secretary) during any period in which the Secretary, the Deputy Secretary of Homeland Security, the Under Secretary for Management, and any officers designated by the Secretary pursuant to 6 U.S.C. 113 to act as Secretary have died, resigned, or otherwise become unable to perform the functions and duties of the office of Secretary, until such time as at least one of the officers mentioned above is able to perform the functions and duties of that office:

- (a) Administrator of the Transportation Security Administration;
- (b) Under Secretary for Intelligence and Analysis;
- (c) Director of the Federal Law Enforcement Training Centers; and
- (d) Region 3 Administrator, Federal Emergency Management Agency.

Sec. 2. Exceptions. (a) No individual who is serving in an office listed in section 1(a)–(d) of this order in an acting capacity shall, by virtue of so serving, act as Secretary pursuant to this order.

(b) No individual who is serving in an office listed in section 1(a)–(d) of this order shall act as Secretary pursuant to this order unless that individual is otherwise eligible to so serve under the Act.

(c) If any individual who is serving in an office listed in section 1(a)–(d) of this order is designated by the Secretary pursuant to 6 U.S.C. 113 to act as Secretary, they shall act as Secretary in accordance with their placement in the order established by the Secretary and not in accordance with their placement on the list in section 1 of this order.

(d) Notwithstanding the provisions of this order, the President retains discretion, to the extent permitted by law, to depart from this order in designating an acting Secretary.

Sec. 3. Revocation. (a) Executive Order 13753 of December 9, 2016 (Amending the Order of Succession in the Department of Homeland Security), is hereby revoked.

(b) Section 88 of Executive Order 13286 of February 28, 2003 (Amendment of Executive Orders, and Other Actions, in Connection With the Transfer of Certain Functions to the Secretary of Homeland Security), is hereby struck in its entirety and the subsequent sections are renumbered accordingly.

Sec. 4. 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) No individual who is serving in an office listed in section 1(a)(i)–(xvii) of this order shall act as Secretary unless that individual is otherwise eligible to so serve under the Act.

(c) Notwithstanding the provisions of this order, the President retains discretion, to the extent permitted by law, to depart from this order in designating an acting Secretary.

Sec. 3. *Revocation.* Executive Order 13612 of May 21, 2012 (Providing an Order of Succession Within the Department of Agriculture), is hereby revoked.

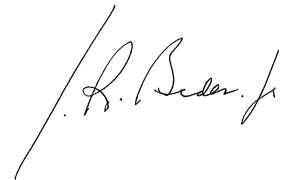
Sec. 4. *General Provisions.* (a) Nothing in this order shall be construed to impair or otherwise affect:

(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.

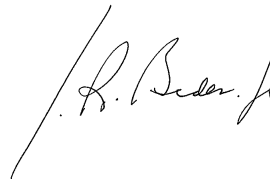
(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.



THE WHITE HOUSE,
January 3, 2025.

(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.



THE WHITE HOUSE,
January 3, 2025.

Presidential Documents

Executive Order 14134 of January 3, 2025

Providing an Order of Succession Within the Department of Agriculture

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the Federal Vacancies Reform Act of 1998, as amended, 5 U.S.C. 3345 *et seq.* (the “Act”), it is hereby ordered that:

Section 1. Order of Succession. (a) Subject to the provisions of section 2 of this order, and to the limitations set forth in the Act, the following officials of the Department of Agriculture, in the order listed, shall act as and perform the functions and duties of the office of Secretary of Agriculture (Secretary) during any period in which both the Secretary and the Deputy Secretary of Agriculture have died, resigned, or otherwise become unable to perform the functions and duties of the office of Secretary:

- (i) Under Secretary of Agriculture for Farm Production and Conservation;
- (ii) Under Secretary of Agriculture for Food, Nutrition, and Consumer Services;
- (iii) Under Secretary of Agriculture for Natural Resources and Environment;
- (iv) Under Secretary of Agriculture for Research, Education, and Economics;
- (v) Under Secretary of Agriculture for Rural Development;
- (vi) Under Secretary of Agriculture for Food Safety;
- (vii) Under Secretary of Agriculture for Marketing and Regulatory Programs;
- (viii) Under Secretary of Agriculture for Trade and Foreign Agricultural Affairs;
- (ix) General Counsel of the Department of Agriculture;
- (x) Assistant Secretary of Agriculture (Congressional Relations and Intergovernmental Affairs);
- (xi) Chief Financial Officer, Department of Agriculture;
- (xii) Assistant Secretary of Agriculture (Civil Rights);
- (xiii) Assistant Secretary of Agriculture (Administration);
- (xiv) Chief of Staff, Office of the Secretary;
- (xv) State Executive Directors of the Farm Service Agency for the States of Kansas, Missouri, and Iowa, in order of seniority fixed by length of unbroken service as State Executive Director of that State;
- (xvi) Director, Office of Budget and Program Analysis; and
- (xvii) Chief, United States Forest Service.

(b) If any two or more individuals designated in subsection (a)(xv) of this section were sworn in to, or commenced service in, their respective offices on the same day, precedence shall be determined by the alphabetical order of the State in which the individual serves.

Sec. 2. Exceptions. (a) No individual who is serving in an office listed in section 1(a)(i)–(xvii) of this order in an acting capacity shall, by virtue of so serving, act as Secretary pursuant to this order.

with investors, project developers, and companies to deliver locally defined benefits to local communities;

(v) increase research and development capacity to accelerate local and regional innovation; or

(vi) strengthen rural, Tribal and community systems.

Sec. 3. *Strengthening Federal Collaboration on Economic Development.* (a) The Secretary of Commerce, acting through the Assistant Secretary for Economic Development and in consultation with the Assistant to the President for Economic Policy, shall, where appropriate and consistent with applicable law, coordinate Federal investments with implementing agencies and develop and implement policy recommendations, including on meaningful community engagement, related to place-based economic development focused on covered communities.

(b) Within 1 year of the date of this order, consistent with applicable law, including section 103 of the Public Works and Economic Development Act of 1965 (42 U.S.C. 3133), the Secretary of Commerce, through the Assistant Secretary for Economic Development, shall work with implementing agencies to:

(i) improve the quality, frequency, and accessibility of engagement with State, Tribal, territorial, local, and non-profit organizations in covered communities;

(ii) support localized, community economic development that helps generate private investments that benefit left-behind communities, such as workforce training, resilient physical infrastructure, affordable energy, civic infrastructure, affordable housing, childcare, and transportation;

(iii) develop an interagency technical assistance network in local geographies to enable interested communities and organizations to access information and resources from across the Federal Government through a single point of entry; and

(v) identify geographies served by overlapping Federal place-based economic development programs to facilitate coordination of funding opportunities and post-award implementation, consistent with applicable law.

(c) Implementing agencies shall, to the extent appropriate and consistent with applicable law, include in forthcoming funding opportunities requirements, application evaluation factors, or incentives that provide a preference for applications from entities in and serving covered communities.

Sec. 4. *Supporting Award Access in Economically Distressed Regions.* (a) Implementing agencies shall, to the extent consistent with applicable law, assist potential grant applicants, including in economically distressed regions, in understanding and applying for Federal grants. Implementing agencies' activities may include:

(i) conducting proactive engagement with communities and organizations to promote opportunities for Federal assistance;

(ii) providing guidance and technical assistance to applicants; and

(iii) identifying resources across the agencies' technical assistance programs and offices for support.

(b) Within 1 year of the date of this order, implementing agencies shall, to the extent consistent with applicable law, consider signing a memorandum of agreement to exchange information, tools, and leading practices to ensure applicants to under-resourced programs are made aware of, and may be considered for, similar programs at other agencies.

Sec. 5. *Promoting Disaster Resilience and Long-Term Economic Development Post-Disaster.* In coordination with the Secretary of Commerce, implementing agencies that have field offices in economically distressed regions or Community Disaster Resilience Zones that have received a major disaster declaration within the past 3 years shall, as appropriate and consistent with applicable law:

(a) seek input from local organizations on needs for and barriers to long-term economic resilience;

(b) identify funding opportunities to address long-term economic development and infrastructure needs; and

(c) provide targeted support for navigating the application process for funding opportunities.

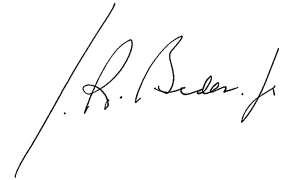
Sec. 6. General Provisions. (a) Nothing in this order shall be construed to impair or otherwise affect:

(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.



THE WHITE HOUSE,
January 19, 2025.

Presidential Documents

Executive Order 14137 of January 3, 2025

Providing an Order of Succession Within the Department of the Treasury

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the Federal Vacancies Reform Act of 1998, as amended, 5 U.S.C. 3345 *et seq.* (the “Act”), it is hereby ordered that:

Section 1. Order of Succession. Subject to the provisions of section 2 of this order, and to the limitations set forth in the Act, the following officials of the Department of the Treasury, in the order listed, shall act as and perform the functions and duties of the office of Secretary of the Treasury (Secretary) during any period in which both the Secretary and the Deputy Secretary of the Treasury have died, resigned, or otherwise become unable to perform the functions and duties of the office of Secretary:

(a) Any Under Secretary of the Treasury, in order of seniority based on date of appointment to such position;

(b) General Counsel for the Department of the Treasury;

(c) Any Deputy Under Secretary of the Treasury or any Assistant Secretary of the Treasury appointed by the President by and with the consent of the Senate, in order of seniority based on date of appointment to such position;

(d) Chief of Staff;

(e) Assistant Secretary of the Treasury for Management;

(f) Fiscal Assistant Secretary;

(g) Commissioner of Internal Revenue, Internal Revenue Service;

(h) Commissioner, Bureau of the Fiscal Service;

(i) Deputy Commissioner, Financing and Operations, Bureau of the Fiscal Service; and

(j) Deputy Commissioner, Internal Revenue Service.

Sec. 2. Exceptions. (a) No individual who is serving in an office listed in section 1(a)–(j) of this order in an acting capacity shall, by virtue of so serving, act as Secretary pursuant to this order.

(b) No individual who is serving in an office listed in section 1(a)–(j) of this order shall act as Secretary unless that individual is otherwise eligible to so serve under the Act.

(c) Notwithstanding the provisions of this order, the President retains discretion, to the extent permitted by law, to depart from this order in designating an acting Secretary.

Sec. 3. Revocation. Executive Order 13735 of August 12, 2016 (Providing an Order of Succession Within the Department of the Treasury), is hereby revoked.

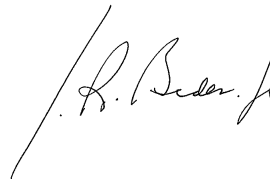
Sec. 4. General Provisions. (a) Nothing in this order shall be construed to impair or otherwise affect:

(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.



THE WHITE HOUSE,
January 3, 2025.