This is historical material "frozen in time". The website is no longer updated
and links to external websites and some internal pages may not work.

JANUARY 16, 2025

Executive Order on 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 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 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

(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 C.F.R. 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 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.

JOSEPH R. BIDEN JR.

THE WHITE HOUSE,

January 16, 2025.