sharing and collaboration among IaaS providers and between IaaS providers and the agencies to inform recommendations under subsection (b) of this section.

(b) Within 240 days of the date of this order, the Attorney General and the Secretary of Homeland Security, in coordination with the Secretary, and, as the Attorney General and Secretary of Homeland Security deem appropriate, the heads of other agencies, shall develop and submit to the President a report containing recommendations to encourage:

(i) voluntary information sharing and collaboration, among United States IaaS providers; and

(ii) information sharing between United States IaaS providers and appropriate agencies, including the reporting of incidents, crimes, and other threats to national security, for the purpose of preventing further harm to the United States.

(c) The report and recommendations provided under subsection (b) of this section shall consider existing mechanisms for such sharing and collaboration, including the Cybersecurity Information Sharing Act [of 2015] (6 U.S.C. 1503 [probably should be ''1501''] *et seq.*), and shall identify any gaps in current law, policy, or procedures. The report shall also include:

(i) information related to the operations of foreign malicious cyber actors, the means by which such actors use IaaS products within the United States, malicious capabilities and tradecraft, and the extent to which persons in the United States are compromised or unwittingly involved in such activity;

(ii) recommendations for liability protections beyond those in existing law that may be needed to encourage United States IaaS providers to share information among each other and with the United States Government; and

(iii) recommendations for facilitating the detection and identification of Accounts and activities that involve foreign malicious cyber actors.

SEC. 4. *Ensuring Sufficient Resources for Implementation.* The Secretary, in consultation with the heads of such agencies as the Secretary deems appropriate, shall identify funding requirements to support the efforts described in this order and incorporate such requirements into its annual budget submissions to the Office of Management and Budget.

SEC. 5. *Definitions.* For the purposes of this order, the following definitions apply:

(a) The term ''entity'' means a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization;

(b) The term ''foreign jurisdiction'' means any country, subnational territory, or region, other than those subject to the civil or military jurisdiction of the United States, in which any person or group of persons exercises sovereign de facto or de jure authority, including any such country, subnational territory, or region in which a person or group of persons is assuming to exercise governmental authority whether such a person or group of persons has or has not been recognized by the United States;

(c) The term ''foreign person'' means a person that is not a United States person;

(d) The term ''Infrastructure as a Service Account'' or ''Account'' means a formal business relationship established to provide IaaS products to a person in which details of such transactions are recorded.

(e) The term ''Infrastructure as a Service Product'' means any product or service offered to a consumer, including complimentary or ''trial'' offerings, that provides processing, storage, networks, or other fundamental computing resources, and with which the consumer is able to deploy and run software that is not predefined, including operating systems and applications. The consumer typically does not manage or control most of the underlying hardware but has control over the operating systems, storage, and any deployed applications. The term is inclusive of ''managed'' products or services, in which the provider is responsible for some aspects of system configuration or maintenance, and ''unmanaged'' products or services, in which the provider is only responsible for ensuring that the product is available to the consumer. The term is also inclusive of ''virtualized'' products and services, in which the computing resources of a physical machine are split between virtualized computers accessible over the internet (e.g., ''virtual private servers''), and ''dedicated'' products or services in which the total computing resources of a physical machine are provided to a single person (e.g., ''bare-metal'' servers);

(f) The term ''malicious cyber-enabled activities'' refers to activities, other than those authorized by or in accordance with United States law that seek to compromise or impair the confidentiality, integrity, or availability of computer, information, or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon;

(g) The term ''person'' means an individual or entity;

(h) The term ''Reseller Account'' means an Infrastructure as a Service Account established to provide IaaS products to a person who will then offer those products subsequently, in whole or in part, to a third party.

(i) The term ''United States Infrastructure as a Service Product'' means any Infrastructure as a Service Product owned by any United States person or operated within the territory of the United States of America;

(j) The term ''United States Infrastructure as a Service Provider'' means any United States Person that offers any Infrastructure as a Service Product;

(k) The term ''United States person'' means any United States citizen, lawful permanent resident of the United States as defined by the Immigration and Nationality Act, entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person located in the United States;

SEC. 6. *Amendment to Reporting Authorizations.* [Amended Ex. Ord. No. 13694, listed in a table under section 1701 of Title 50, War and National Defense.]

SEC. 7. *General Provisions.* (a) The Secretary, in consultation with the heads of such other agencies as the Secretary deems appropriate, is hereby authorized to take such actions, including the promulgation of rules and regulations, and employ all powers granted to the President by IEEPA as may be necessary to carry out the purposes of this order. The Secretary may redelegate any of these functions to other officers within the Department of Commerce, consistent with applicable law. All departments and agencies of the United States Government are hereby directed to take all appropriate measures within their authority to carry out the provisions of this order.

(b) 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.

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

(d) Nothing in this order prohibits or otherwise restricts authorized intelligence, military, law enforcement, or other activities in furtherance of national security or public safety activities.

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

DONALD J. TRUMP.

§ 7422. No regulatory authority

Nothing in this chapter shall be construed to confer any regulatory authority on any Federal, State, tribal, or local department or agency.

(Pub. L. 113–274, § 3, Dec. 18, 2014, 128 Stat. 2972.)

Editorial Notes

REFERENCES IN TEXT

This chapter, referred to in text, was in the original ''this Act'', meaning Pub. L. 113–274, Dec. 18, 2014, 128 Stat. 2971, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 7421 of this title and Tables.

§ 7423. No additional funds authorized

No additional funds are authorized to carry out this Act, and the amendments made by this Act. This Act, and the amendments made by this Act, shall be carried out using amounts otherwise authorized or appropriated.

(Pub. L. 113–274, § 4, Dec. 18, 2014, 128 Stat. 2972.)

Editorial Notes

REFERENCES IN TEXT

This Act, and the amendments made by this Act, referred to in text, is Pub. L. 113–274, Dec. 18, 2014, 128 Stat. 2971, which enacted this chapter and amended sections 272, 278g–3, 7403, and 7406 of this title. For complete classification of this Act to the Code, see Short Title note set out under section 7421 of this title and Tables.

SUBCHAPTER I—CYBERSECURITY RESEARCH AND DEVELOPMENT

§ 7431. Federal cybersecurity research and development

(a) Fundamental cybersecurity research

(1) Federal cybersecurity research and development strategic plan

The heads of the applicable agencies and departments, working through the National Science and Technology Council and the Networking and Information Technology Research and Development Program, shall develop and update every 4 years a Federal cybersecurity research and development strategic plan (referred to in this subsection as the ''strategic plan'') based on an assessment of cybersecurity risk to guide the overall direction of Federal cybersecurity and information assurance research and development for information technology and networking systems. The heads of the applicable agencies and departments shall build upon existing programs and plans to develop the strategic plan to meet objectives in cybersecurity, such as—

(A) how to design and build complex software-intensive systems that are secure and reliable when first deployed;

(B) how to test and verify that software and hardware, whether developed locally or obtained from a third party, is free of significant known security flaws;

(C) how to test and verify that software and hardware obtained from a third party correctly implements stated functionality, and only that functionality;

(D) how to guarantee the privacy of an individual, including that individual's identity, information, and lawful transactions when stored in distributed systems or transmitted over networks;

(E) how to build new protocols to enable the Internet to have robust security as one of the key capabilities of the Internet;

(F) how to determine the origin of a message transmitted over the Internet;

(G) how to support privacy in conjunction with improved security;

(H) how to address the problem of insider threats;

(I) how improved consumer education and digital literacy initiatives can address human factors that contribute to cybersecurity;

(J) how to protect information processed, transmitted, or stored using cloud computing or transmitted through wireless services;

(K) implementation of section 7432 of this title through research and development on the topics identified under subsection (a) of such section; and

(L) any additional objectives the heads of the applicable agencies and departments, in coordination with the head of any relevant Federal agency and with input from stakeholders, including appropriate national laboratories, industry, and academia, determine appropriate.

(2) Requirements

(A) Contents of plan

The strategic plan shall—

(i) specify and prioritize near-term, mid-term, and long-term research objectives, including objectives associated with the research identified in section 7403(a)(1) of this title;

(ii) specify how the near-term objectives described in clause (i) complement research and development areas in which the private sector is actively engaged;

(iii) describe how the heads of the applicable agencies and departments will focus on innovative, transformational technologies with the potential to enhance the security, reliability, resilience, and trustworthiness of the digital infrastructure, and to protect consumer privacy;

(iv) describe how the heads of the applicable agencies and departments will foster the rapid transfer of research and development results into new cybersecurity technologies and applications for the timely benefit of society and the national interest, including through the dissemination of best practices and other outreach activities;

(v) describe how the heads of the applicable agencies and departments will establish and maintain a national research infrastructure for creating, testing, and evaluating the next generation of secure networking and information technology systems; and

(vi) describe how the heads of the applicable agencies and departments will facilitate access by academic researchers to the infrastructure described in clause (v), as well as to relevant data, including event data.

(B) Private sector efforts

In developing, implementing, and updating the strategic plan, the heads of the applica-