puting 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;