Executive Order 13984—Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities

January 19, 2021

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), and section 301 of title 3, United States Code:

I, Donald J. Trump, President of the United States of America, find that additional steps must be taken to deal with the national emergency related 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, to address the use of United States Infrastructure as a Service (IaaS) products by foreign malicious cyber actors. IaaS products provide persons the ability to run software and store data on servers offered for rent or lease without responsibility for the maintenance and operating costs of those servers. Foreign malicious cyber actors aim to harm the United States economy through the theft of intellectual property and sensitive data and to threaten national security by targeting United States critical infrastructure for malicious cyber-enabled activities. Foreign actors use United States IaaS products for a variety of tasks in carrying out malicious cyber-enabled activities, which makes it extremely difficult for United States officials to track and obtain information through legal process before these foreign actors transition to replacement infrastructure and destroy evidence of their prior activities; foreign resellers of United States IaaS products make it easier for foreign actors to access these products and evade detection. This order provides authority to impose record-keeping obligations with respect to foreign transactions. To address these threats, to deter foreign malicious cyber actors' use of United States IaaS products, and to assist in the investigation of transactions involving foreign malicious cyber actors, the United States must ensure that providers offering United States IaaS products verify the identity of persons obtaining an IaaS account ("Account") for the provision of these products and maintain records of those transactions. In appropriate circumstances, to further protect against malicious cyber-enabled activities, the United States must also limit certain foreign actors' access to United States IaaS products. Further, the United States must encourage more robust cooperation among United States IaaS providers, including by increasing voluntary information sharing, to bolster efforts to thwart the actions of foreign malicious cyber actors.

Accordingly, I hereby order:

Section 1. *Verification of Identity*. Within 180 days of the date of this order, the Secretary of Commerce (Secretary) shall propose for notice and comment regulations that require United States IaaS providers to verify the identity of a foreign person that obtains an Account. These regulations shall, at a minimum:

(a) set forth the minimum standards that United States IaaS providers must adopt to verify the identity of a foreign person in connection with the opening of an Account or the maintenance of an existing Account, including:

> (i) the types of documentation and procedures required to verify the identity of any foreign person acting as a lessee or sub-lessee of these products or services;
>
> (ii) records that United States IaaS providers must securely maintain regarding a foreign person that obtains an Account, including information establishing:

(A) the identity of such foreign person and the person's information, including name, national identification number, and address;

(B) means and source of payment (including any associated financial institution and other identifiers such as credit card number, account number, customer identifier, transaction identifiers, or virtual currency wallet or wallet address identifier);

(C) electronic mail address and telephonic contact information, used to verify a foreign person's identity; and

(D) Internet Protocol addresses used for access or administration and the date and time of each such access or administrative action, related to ongoing verification of such foreign person's ownership of such an Account; and

(iii) methods for limiting all third-party access to the information described in this subsection, except insofar as such access is otherwise consistent with this order and allowed under applicable law;

(b) take into consideration the type of Account maintained by United States IaaS providers, methods of opening an Account, and types of identifying information available to accomplish the objectives of identifying foreign malicious cyber actors using any such products and avoiding the imposition of an undue burden on such providers; and

(c) permit the Secretary, in accordance with such standards and procedures as the Secretary may delineate and in consultation with the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence, to exempt any United States IaaS provider, or any specific type of Account or lessee, from the requirements of any regulation issued pursuant to this section. Such standards and procedures may include a finding by the Secretary that a provider, Account, or lessee complies with security best practices to otherwise deter abuse of IaaS products.

Sec. 2. *Special Measures for Certain Foreign Jurisdictions or Foreign Persons*. (a) Within 180 days of the date of this order, the Secretary shall propose for notice and comment regulations that require United States IaaS providers to take any of the special measures described in subsection (d) of this section if the Secretary, in consultation with the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the Director of National Intelligence and, as the Secretary deems appropriate, the heads of other executive departments and agencies (agencies), finds:

(i) that reasonable grounds exist for concluding that a foreign jurisdiction has any significant number of foreign persons offering United States IaaS products that are used for malicious cyber-enabled activities or any significant number of foreign persons directly obtaining United States IaaS products for use in malicious cyber-enabled activities, in accordance with subsection (b) of this section; or

(ii) that reasonable grounds exist for concluding that a foreign person has established a pattern of conduct of offering United States IaaS products that are used for malicious cyber-enabled activities or directly obtaining United States IaaS products for use in malicious cyber-enabled activities.

(b) In making findings under subsection (a) of this section on the use of United States IaaS products in malicious cyber-enabled activities, the Secretary shall consider any information the Secretary determines to be relevant, as well as information pertaining to the following factors:

(i) Factors related to a particular foreign jurisdiction, including:

(A) evidence that foreign malicious cyber actors have obtained United States IaaS products from persons offering United States IaaS products in that foreign jurisdiction, including whether such actors obtained such IaaS products through Reseller Accounts;

(B) the extent to which that foreign jurisdiction is a source of malicious cyber-enabled activities; and

(C) Whether the United States has a mutual legal assistance treaty with that foreign jurisdiction, and the experience of United States law enforcement officials and regulatory officials in obtaining information about activities involving United States IaaS products originating in or routed through such foreign jurisdiction; and

(ii) Factors related to a particular foreign person, including:

(A) the extent to which a foreign person uses United States IaaS products to conduct, facilitate, or promote malicious cyber-enabled activities;

(B) the extent to which United States IaaS products offered by a foreign person are used to facilitate or promote malicious cyber-enabled activities;

(C) the extent to which United States IaaS products offered by a foreign person are used for legitimate business purposes in the jurisdiction; and

(D) the extent to which actions short of the imposition of special measures pursuant to subsection (d) of this section are sufficient, with respect to transactions involving the foreign person offering United States IaaS products, to guard against malicious cyber-enabled activities.

(c) In selecting which special measure or measures to take under this section, the Secretary shall consider:

(i) whether the imposition of any special measure would create a significant competitive disadvantage, including any undue cost or burden associated with compliance, for United States IaaS providers;

(ii) the extent to which the imposition of any special measure or the timing of the special measure would have a significant adverse effect on legitimate business activities involving the particular foreign jurisdiction or foreign person; and

(iii) the effect of any special measure on United States national security, law enforcement investigations, or foreign policy.

(d) The special measures referred to in subsections (a), (b), and (c) of this section are as follows:

(i) Prohibitions or Conditions on Accounts within Certain Foreign Jurisdictions: The Secretary may prohibit or impose conditions on the opening or maintaining with any United States IaaS provider of an Account, including a Reseller Account, by any foreign person located in a foreign jurisdiction found to have any significant number of foreign persons offering United States IaaS products used for malicious cyber-enabled activities, or by any United States IaaS provider for or on behalf of a foreign person; and

(ii) Prohibitions or Conditions on Certain Foreign Persons: The Secretary may prohibit or impose conditions on the opening or maintaining in the United States of an Account, including a Reseller Account, by any United States IaaS provider for or on behalf of a foreign person, if such an Account involves any such foreign person found to be

offering United States IaaS products used in malicious cyber-enabled activities or directly obtaining United States IaaS products for use in malicious cyber-enabled activities.

(e) The Secretary shall not impose requirements for United States IaaS providers to take any of the special measures described in subsection (d) of this section earlier than 180 days following the issuance of final regulations described in section 1 of this order.

Sec. 3. *Recommendations for Cooperative Efforts to Deter the Abuse of United States IaaS Products*. (a) Within 120 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 the Secretary of Homeland Security deem appropriate, the heads of other agencies, shall engage and solicit feedback from industry on how to increase information 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 (6 U.S.C. 1503 *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. Section (9) of Executive Order 13694, as amended, is further amended to read as follows:

"Sec. 9. The Secretary of the Treasury, in consultation with the Secretary of State, the Attorney General, and the Secretary of Commerce, is hereby authorized to submit the recurring and final reports to the Congress on the national emergency declared in this order, consistent with section 401(c) of the NEA (50 U.S.C. 1641(c)) and section 204(c) of IEEPA (50 U.S.C. 1703(c))."

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

The White House,
January 19, 2021.

[Filed with the Office of the Federal Register, 8:45 a.m., January 22, 2021]

NOTE: This Executive order was published in the *Federal Register* on January 25.

Categories: Executive Orders : Malicious cyber-enabled activities, additional steps to address national emergency.

Subjects: Defense and national security : Cybersecurity :: Strengthening efforts.

DCPD Number: DCPD202100042.