Federal Register
Vol. 84, No. 96
Friday, May 17, 2019

Presidential Documents

Title 3—

The President

Executive Order 13873 of May 15, 2019

Securing the Information and Communications Technology and Services Supply Chain

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.*), and section 301 of title 3, United States Code,

I, DONALD J. TRUMP, President of the United States of America, find that foreign adversaries are increasingly creating and exploiting vulnerabilities in information and communications technology and services, which store and communicate vast amounts of sensitive information, facilitate the digital economy, and support critical infrastructure and vital emergency services, in order to commit malicious cyber-enabled actions, including economic and industrial espionage against the United States and its people. I further find that the unrestricted acquisition or use in the United States of information and communications technology or services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries augments the ability of foreign adversaries to create and exploit vulnerabilities in information and communications technology or services, with potentially catastrophic effects, and thereby constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States. This threat exists both in the case of individual acquisitions or uses of such technology or services, and when acquisitions or uses of such technologies are considered as a class. Although maintaining an open investment climate in information and communications technology, and in the United States economy more generally, is important for the overall growth and prosperity of the United States, such openness must be balanced by the need to protect our country against critical national security threats. To deal with this threat, additional steps are required to protect the security, integrity, and reliability of information and communications technology and services provided and used in the United States. In light of these findings, I hereby declare a national emergency with respect to this threat.

Accordingly, it is hereby ordered as follows:

Section 1. *Implementation.* (a) The following actions are prohibited: any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service (transaction) by any person, or with respect to any property, subject to the jurisdiction of the United States, where the transaction involves any property in which any foreign country or a national thereof has any interest (including through an interest in a contract for the provision of the technology or service), where the transaction was initiated, is pending, or will be completed after the date of this order, and where the Secretary of Commerce (Secretary), in consultation with the Secretary of the Treasury, the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the United States Trade Representative, the Director of National Intelligence, the Administrator of General Services, the Chairman of the Federal Communications Commission, and, as appropriate, the heads of other executive departments and agencies (agencies), has determined that:

(i) the transaction involves information and communications technology or services designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary; and

(ii) the transaction:

(A) poses an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of information and communications technology or services in the United States;

(B) poses an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the digital economy of the United States; or

(C) otherwise poses an unacceptable risk to the national security of the United States or the security and safety of United States persons.

(b) The Secretary, in consultation with the heads of other agencies as appropriate, may at the Secretary's discretion design or negotiate measures to mitigate concerns identified under section 1(a) of this order. Such measures may serve as a precondition to the approval of a transaction or of a class of transactions that would otherwise be prohibited pursuant to this order.

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

Sec. 2. *Authorities.* (a) The Secretary, in consultation with, or upon referral of a particular transaction from, the heads of other agencies as appropriate, is hereby authorized to take such actions, including directing the timing and manner of the cessation of transactions prohibited pursuant to section 1 of this order, adopting appropriate rules and regulations, and employing all other powers granted to the President by IEEPA, as may be necessary to implement this order. All agencies of the United States Government are directed to take all appropriate measures within their authority to carry out the provisions of this order.

(b) Rules and regulations issued pursuant to this order may, among other things, determine that particular countries or persons are foreign adversaries for the purposes of this order; identify persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries for the purposes of this order; identify particular technologies or countries with respect to which transactions involving information and communications technology or services warrant particular scrutiny under the provisions of this order; establish procedures to license transactions otherwise prohibited pursuant to this order; establish criteria, consistent with section 1 of this order, by which particular technologies or particular participants in the market for information and communications technology or services may be recognized as categorically included in or as categorically excluded from the prohibitions established by this order; and identify a mechanism and relevant factors for the negotiation of agreements to mitigate concerns raised in connection with subsection 1(a) of this order. Within 150 days of the date of this order, the Secretary, in consultation with the Secretary of the Treasury, Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the United States Trade Representative, the Director of National Intelligence, the Administrator of General Services, the Chairman of the Federal Communications Commission and, as appropriate, the heads of other agencies, shall publish rules or regulations implementing the authorities delegated to the Secretary by this order.

(c) The Secretary may, consistent with applicable law, redelegate any of the authorities conferred on the Secretary pursuant to this section within the Department of Commerce.

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

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

(b) the term ''foreign adversary'' means any foreign government or foreign non-government person engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons;

(c) the term ''information and communications technology or services'' means any hardware, software, or other product or service primarily intended to fulfill or enable the function of information or data processing, storage, retrieval, or communication by electronic means, including transmission, storage, and display;

(d) the term ''person'' means an individual or entity; and

(e) the term ''United States person'' means any United States citizen, permanent resident alien, entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person in the United States.

Sec. 4. Recurring and Final Reports to the Congress. The Secretary, in consultation with the Secretary of State, is hereby authorized to submit 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. 5. *Assessments and Reports.* (a) The Director of National Intelligence shall continue to assess threats to the United States and its people from information and communications technology or services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary. The Director of National Intelligence shall produce periodic written assessments of these threats in consultation with the heads of relevant agencies, and shall provide these assessments to the President, the Secretary for the Secretary's use in connection with his responsibilities pursuant to this order, and the heads of other agencies as appropriate. An initial assessment shall be completed within 40 days of the date of this order, and further assessments shall be completed at least annually, and shall include analysis of:

(i) threats enabled by information and communications technologies or services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary; and

(ii) threats to the United States Government, United States critical infrastructure, and United States entities from information and communications technologies or services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the influence of a foreign adversary.

(b) The Secretary of Homeland Security shall continue to assess and identify entities, hardware, software, and services that present vulnerabilities in the United States and that pose the greatest potential consequences to the national security of the United States. The Secretary of Homeland Security, in coordination with sector-specific agencies and coordinating councils as appropriate, shall produce a written assessment within 80 days of the date of this order, and annually thereafter. This assessment shall include an evaluation of hardware, software, or services that are relied upon by multiple information and communications technology or service providers, including the communication services relied upon by critical infrastructure entities identified pursuant to section 9 of Executive Order 13636 of February 12, 2013 (Improving Critical Infrastructure Cybersecurity).

(c) Within 1 year of the date of this order, and annually thereafter, the Secretary, in consultation as appropriate with the Secretary of the Treasury, the Secretary of Homeland Security, Secretary of State, the Secretary of Defense, the Attorney General, the United States Trade Representative, the

Director of National Intelligence, and the Chairman of the Federal Communications Commission, shall assess and report to the President whether the actions taken by the Secretary pursuant to this order are sufficient and continue to be necessary to mitigate the risks identified in, and pursuant to, this order.

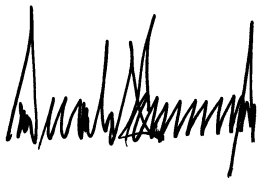
Sec. 6. *General Provisions.* (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

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

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



THE WHITE HOUSE,
May 15, 2019.

[FR Doc. 2019–10538
Filed 5–16–19; 11:15 am]
Billing code 3295–F9–P