Executive Order 14034—Protecting Americans' Sensitive Data From Foreign Adversaries

June 9, 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*.), and section 301 of title 3, United States Code,

I, Joseph R. Biden Jr., President of the United States of America, find that it is appropriate to elaborate upon measures to address the national emergency with respect to the information and communications technology and services supply chain that was declared in Executive Order 13873 of May 15, 2019 (Securing the Information and Communications Technology and Services Supply Chain). Specifically, the increased use in the United States of certain connected software applications designed, developed, manufactured, or supplied by persons owned or controlled by, or subject to the jurisdiction or direction of, a foreign adversary, which the Secretary of Commerce acting pursuant to Executive Order 13873 has defined to include the People's Republic of China, among others, continues to threaten the national security, foreign policy, and economy of the United States. The Federal Government should evaluate these threats through rigorous, evidence-based analysis and should address any unacceptable or undue risks consistent with overall national security, foreign policy, and economic objectives, including the preservation and demonstration of America's core values and fundamental freedoms.

By operating on United States information and communications technology devices, including personal electronic devices such as smartphones, tablets, and computers, connected software applications can access and capture vast swaths of information from users, including United States persons' personal information and proprietary business information. This data collection threatens to provide foreign adversaries with access to that information. Foreign adversary access to large repositories of United States persons' data also presents a significant risk.

In evaluating the risks of a connected software application, several factors should be considered. Consistent with the criteria established in Executive Order 13873, and in addition to the criteria set forth in implementing regulations, potential indicators of risk relating to connected software applications include: ownership, control, or management by persons that support a foreign adversary's military, intelligence, or proliferation activities; use of the connected software application to conduct surveillance that enables espionage, including through a foreign adversary's access to sensitive or confidential government or business information, or sensitive personal data; ownership, control, or management of connected software applications by persons subject to coercion or cooption by a foreign adversary; ownership, control, or management of connected software applications by persons involved in malicious cyber activities; a lack of thorough and reliable third-party auditing of connected software applications; the scope and sensitivity of the data collected; the number and sensitivity of the users of the connected software application; and the extent to which identified risks have been or can be addressed by independently verifiable measures.

The ongoing emergency declared in Executive Order 13873 arises from a variety of factors, including the continuing effort of foreign adversaries to steal or otherwise obtain United States persons' data. That continuing effort by foreign adversaries constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States. To

address this threat, the United States must act to protect against the risks associated with connected software applications that are designed, developed, manufactured, or supplied by persons owned or controlled by, or subject to the jurisdiction or direction of, a foreign adversary.

Additionally, the United States seeks to promote accountability for persons who engage in serious human rights abuse. If persons who own, control, or manage connected software applications engage in serious human rights abuse or otherwise facilitate such abuse, the United States may impose consequences on those persons in action separate from this order.

Accordingly, it is hereby ordered that:

Section 1. *Revocation of Presidential Actions*. The following orders are revoked: Executive Order 13942 of August 6, 2020 (Addressing the Threat Posed by TikTok, and Taking Additional Steps To Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain); Executive Order 13943 of August 6, 2020 (Addressing the Threat Posed by WeChat, and Taking Additional Steps To Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain); and Executive Order 13971 of January 5, 2021 (Addressing the Threat Posed by Applications and Other Software Developed or Controlled by Chinese Companies).

Sec. 2. *Implementation*. (a) The Director of the Office of Management and Budget and the heads of executive departments and agencies (agencies) shall promptly take steps to rescind any orders, rules, regulations, guidelines, or policies, or portions thereof, implementing or enforcing Executive Orders 13942, 13943, or 13971, as appropriate and consistent with applicable law, including the Administrative Procedure Act, 5 U.S.C. 551 *et seq*. In addition, any personnel positions, committees, task forces, or other entities established pursuant to Executive Orders 13942, 13943, or 13971 shall be abolished, as appropriate and consistent with applicable law.

(b) Not later than 120 days after the date of this order, the Secretary of Commerce, in consultation with the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Health and Human Services, the Secretary of Homeland Security, the Director of National Intelligence, and the heads of other agencies as the Secretary of Commerce deems appropriate, shall provide a report to the Assistant to the President and National Security Advisor with recommendations to protect against harm from the unrestricted sale of, transfer of, or access to United States persons' sensitive data, including personally identifiable information, personal health information, and genetic information, and harm from access to large data repositories by persons owned or controlled by, or subject to the jurisdiction or direction of, a foreign adversary. Not later than 60 days after the date of this order, the Director of National Intelligence shall provide threat assessments, and the Secretary of Homeland Security shall provide vulnerability assessments, to the Secretary of Commerce to support development of the report required by this subsection.

(c) Not later than 180 days after the date of this order, the Secretary of Commerce, in consultation with the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the Director of the Office of Management and Budget, and the heads of other agencies as the Secretary of Commerce deems appropriate, shall provide a report to the Assistant to the President and National Security Advisor recommending additional executive and legislative actions to address the risk associated with connected software applications that are designed, developed, manufactured, or supplied by persons owned or controlled by, or subject to the jurisdiction or direction of, a foreign adversary.

(d) The Secretary of Commerce shall evaluate on a continuing basis transactions involving connected software applications that may pose an undue risk of sabotage or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance

of information and communications technology or services in the United States; pose an undue risk of catastrophic effects on the security or resiliency of the critical infrastructure or digital economy of the United States; or otherwise pose an unacceptable risk to the national security of the United States or the security and safety of United States persons. Based on the evaluation, the Secretary of Commerce shall take appropriate action in accordance with Executive Order 13873 and its implementing regulations.

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

(a) the term "connected software application" means software, a software program, or a group of software programs, that is designed to be used on an end-point computing device and includes as an integral functionality, the ability to collect, process, or transmit data via the Internet;

(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, lawful permanent resident, 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. *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.

JOSEPH R. BIDEN, JR.

The White House,
June 9, 2021.

[Filed with the Office of the Federal Register, 11:15 a.m., June 10, 2021]

NOTE: This Executive order was published in the *Federal Register* on June 11.

Categories: Executive Orders : Sensitive consumer data, protection efforts from foreign adversaries.

Subjects: Business and industry : Consumer data security, strengthening efforts.

DCPD Number: DCPD202100490.