MARCH 27, 2023

Executive Order on Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. Technology is central to the future of our national

security, economy, and democracy. The United States has fundamental national security and foreign policy interests in (1) ensuring that technology is developed, deployed, and governed in accordance with universal human rights; the rule of law; and appropriate legal authorization, safeguards, and oversight, such that it supports, and does not undermine, democracy, civil rights and civil liberties, and public safety; and (2) mitigating, to the greatest extent possible, the risk emerging technologies may pose to United States Government institutions, personnel, information, and information systems.

To advance these interests, the United States supports the development of an international technology ecosystem that protects the integrity of international standards development; enables and promotes the free flow of data and ideas with trust; protects our security, privacy, and human rights; and enhances our economic competitiveness. The growing exploitation of Americans' sensitive data and improper use of surveillance

technology, including commercial spyware, threatens the development of this ecosystem. Foreign governments and persons have deployed commercial spyware against United States Government institutions, personnel, information, and information systems, presenting significant counterintelligence and security risks to the United States Government. Foreign governments and persons have also used commercial spyware for improper purposes, such as to target and intimidate perceived opponents; curb dissent; limit freedoms of expression, peaceful assembly, or association; enable other human rights abuses or suppression of civil liberties; and track or target United States persons without proper legal authorization, safeguards, or oversight.

The United States has a fundamental national security and foreign policy interest in countering and preventing the proliferation of commercial spyware that has been or risks being misused for such purposes, in light of the core interests of the United States in protecting United States Government personnel and

United States citizens around the world; upholding and advancing democracy; promoting respect for human rights; and defending activists, dissidents, and journalists against threats to their freedom and dignity. To advance these interests and promote responsible use of commercial spyware, the United States must establish robust protections and procedures to ensure that any United States Government use of commercial spyware helps protect its information systems and intelligence and law enforcement activities against significant counterintelligence or security risks; aligns with its core interests in promoting democracy and democratic values around the world; and ensures that the United States Government does not contribute, directly or indirectly, to the proliferation of commercial spyware that has been misused by foreign governments or facilitate such misuse.

Therefore, I hereby establish as the policy of the United States Government that it shall not make operational use of commercial spyware that poses significant

counterintelligence or security risks to the United States Government or significant risks of improper use by a foreign government or foreign person. In furtherance of the national security and foreign policy interests of the United States, this order accordingly directs steps to implement that policy and protect the safety and security of United States Government institutions, personnel, information, and information systems; discourage the improper use of commercial spyware; and encourage the development and implementation of responsible norms regarding the use of commercial spyware that are consistent with respect for the rule of law, human rights, and democratic norms and values. The actions directed in this order are consistent with the policy objectives set forth in section 6318 of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 (NDAA FY 2023) (Public Law 117-263) and section 5502 of the National Defense Authorization Act for Fiscal Year 2022 (NDAA FY 2022) (Public Law 117-81).

Sec. 2. Prohibition on Operational Use. (a) Executive departments and

agencies (agencies) shall not make operational use of commercial spyware where they determine, based on credible information, that such use poses significant counterintelligence or security risks to the United States Government or that the commercial spyware poses significant risks of improper use by a foreign government or foreign person. For the purposes of this use prohibition:

(i) Commercial spyware may pose counterintelligence or security risks to the United States Government when:

(A) a foreign government or foreign person has used or acquired the commercial spyware to gain or attempt to gain access to United States Government computers or the computers of United States Government personnel without authorization from the United States Government; or

(B) the commercial spyware was or is furnished by an entity that:

(1) maintains, transfers, or uses data obtained from the

commercial spyware without authorization from the licensed end-user or the United States Government;

(2) has disclosed or intends to disclose non-public United States Government information or non-public information about the activities of the United States Government without authorization from the United States Government; or

(3) is under the direct or effective control of a foreign government or foreign person engaged in intelligence activities, including surveillance or espionage, directed against the United States.

(ii) Commercial spyware may pose risks of improper use by a foreign government or foreign person when:

(A) the commercial spyware, or other commercial spyware furnished by the same vendor, has been used by a foreign government or foreign person for any of the following purposes:

(1) to collect information on activists, academics, journalists,

dissidents, political figures, or members of non-governmental organizations or marginalized communities in order to intimidate such persons; curb dissent or political opposition; otherwise limit freedoms of expression, peaceful assembly, or association; or enable other forms of human rights abuses or suppression of civil liberties; or

(2) to monitor a United States person, without such person's consent, in order to facilitate the tracking or targeting of the person without proper legal authorization, safeguards, and oversight; or

(B) the commercial spyware was furnished by an entity that provides commercial spyware to governments for which there are credible reports in the annual country reports on human rights practices of the Department of State that they engage in systematic acts of political repression, including arbitrary arrest or detention, torture, extrajudicial or politically motivated killing, or other gross violations of human rights, consistent with any findings by the Department of State pursuant to

section 5502 of the NDAA FY 2022 or other similar findings.

(iii) In determining whether the operational use of commercial spyware poses significant counterintelligence or security risks to the United States Government or poses significant risks of improper use by a foreign government or foreign person, such that operational use should be prohibited, agencies shall consider, among other relevant considerations, whether the entity furnishing the commercial spyware knew or reasonably should have known that the spyware posed risks described in subsections (a)(i) or (ii) of this section, and whether the entity has taken appropriate measures to remove such risks, such as canceling relevant licensing agreements or contracts that present such risks; taking other verifiable action to prevent continuing uses that present such risks; or cooperating in United States Government efforts to counter improper use of the spyware.

(b) An agency shall not request or directly enable a third party to make operational use of commercial

spyware where the agency has determined that such use poses significant counterintelligence or security risks to the United States Government or that the commercial spyware poses significant risks of improper use by a foreign government or foreign person, as described in subsection (a) of this section. For purposes of this order, the term "operational use" includes such indirect use.

(c) To facilitate effective interagency coordination of information relevant to the factors set forth in subsection (a) of this section and to promote consistency of application of this order across the United States Government, the Director of National Intelligence (DNI) shall, within 90 days of the date of this order, and on a semiannual basis thereafter, issue a classified intelligence assessment that integrates relevant information — including intelligence, open source, financial, sanctions-related, and export controls-related information — on foreign commercial spyware or foreign government or foreign person use of commercial spyware relevant to

the factors set forth in subsection (a) of this section. The intelligence assessment shall incorporate, but not be limited to, the report and assessment required by section 1102A(b) of the National Security Act of 1947, 50 U.S.C. 3001 *et seq*., as amended by section 6318(c) of the NDAA FY 2023. In order to facilitate the production of the intelligence assessment, the head of each agency shall, on an ongoing basis, provide the DNI all new credible information obtained by the agency on foreign commercial spyware vendors or foreign government or foreign person use of commercial spyware relevant to the factors set forth in subsection (a) of this section. Such information shall include intelligence, open source, financial, sanctions-related, export controls-related, and due diligence information, as well as information relevant to the development of the list of covered contractors developed or maintained pursuant to section 5502 of the NDAA FY 2022 or other similar information.

(d) Any agency that makes a determination of whether operational use of a commercial spyware product

is prohibited under subsection (a) of this section shall provide the results of that determination and key elements of the underlying analysis to the DNI. After consulting with the submitting agency to protect operational sensitivities, the DNI shall incorporate this information into the intelligence assessment described in subsection (c) of this section and, as needed, shall make this information available to other agencies consistent with section 3(b) of this order.

(e) The Assistant to the President for National Security Affairs (APNSA), or a designee, shall, within 30 days of the issuance of the intelligence assessment described in subsection (c) of this section, and additionally as the APNSA or designee deems necessary, convene agencies to discuss the intelligence assessment, as well as any other information about commercial spyware relevant to the factors set forth in subsection (a) of this section, in order to ensure effective interagency awareness and sharing of such information.

(f) For any commercial spyware intended by an agency for operational

use, a relevant official, as provided in section 5(k) of this order, shall certify the determination that the commercial spyware does not pose significant counterintelligence or security risks to the United States Government or significant risks of improper use by a foreign government or foreign person based on the factors set forth in subsection (a) of this section. The obligation to certify such a determination shall not be delegated, except as provided in section 5(k) of this order.

(g) If an agency decides to make operational use of commercial spyware, the head of the agency shall notify the APNSA of such decision, describing the due diligence completed before the decision was made, providing relevant information on the agency's consideration of the factors set forth in subsection (a) of this section, and providing the reasons for the agency's determination. The agency may not make operational use of the commercial spyware until at least 7 days after providing this information or until the APNSA has notified the agency that no further process is required.

(h) Within 90 days of the issuance of the intelligence assessment described in subsection (c) of this section, each agency shall review all existing operational uses of commercial spyware and discontinue, as soon as the head of the agency determines is reasonably possible without compromising ongoing operations, operational use of any commercial spyware that the agency determines poses significant counterintelligence or security risks to the United States Government or significant risks of improper use by a foreign government or foreign person, pursuant to subsection (a) of this section.

(i) Within 180 days of the date of this order, each agency that may make operational use of commercial spyware shall develop appropriate internal controls and oversight procedures for conducting determinations under subsection (a) of this section, as appropriate and consistent with applicable law.

(j) At any time after procuring commercial spyware for operational

use, if the agency obtains relevant information with respect to the factors set forth in subsection (a) of this section, the agency shall determine whether the commercial spyware poses significant counterintelligence or security risks to the United States Government or significant risks of improper use by a foreign government or foreign person, and, if so, shall terminate such operational use as soon as the head of the agency determines is reasonably possible without compromising ongoing operations, and shall notify the DNI and the APNSA.

(k) The Federal Acquisition Security Council shall consider the intelligence assessment described in subsection (c) of this section in evaluating whether commercial spyware poses a supply chain risk, as appropriate and consistent with applicable law, including 41 C.F.R. Part 201-1 and 41 U.S.C. 1323.

(l) The prohibitions contained in this section shall not apply to the use of commercial spyware for purposes of testing, research, analysis, cybersecurity, or the development of

countermeasures for counterintelligence or security risks, or for purposes of a criminal investigation arising out of the criminal sale or use of the spyware.

(m) A relevant official, as provided in section 5(k) of this order, may issue a waiver, for a period not to exceed 1 year, of an operational use prohibition determined pursuant to subsection (a) of this section if the relevant official determines that such waiver is necessary due to extraordinary circumstances and that no feasible alternative is available to address such circumstances. This authority shall not be delegated, except as provided in section 5(k) of this order. A relevant official may, at any time, revoke any waiver previously granted. Within 72 hours of making a determination to issue or revoke a waiver pursuant to this subsection, the relevant official who has issued or revoked the waiver shall notify the President, through the APNSA, of this determination, including the justification for the determination. The relevant official shall provide this information concurrently to the DNI.

Sec. 3. Application to Procurement. An agency seeking to procure commercial spyware for any purpose other than for a criminal investigation arising out of the criminal sale or use of the spyware shall, prior to making such procurement and consistent with its existing statutory and regulatory authorities:

(a) review the intelligence assessment issued by the DNI pursuant to section 2(c) of this order;

(b) request from the DNI any additional information regarding the commercial spyware that is relevant to the factors set forth in section 2(a) of this order;

(c) consider the factors set forth in section 2(a) of this order in light of the information provided by the DNI; and

(d) consider whether any entity furnishing the commercial spyware being considered for procurement has implemented reasonable due diligence procedures and standards — such as the industry-wide norms reflected in relevant Department of State guidance

on business and human rights and on transactions linked to foreign government end-users for products or services with surveillance capabilities — and controls that would enable the entity to identify and prevent uses of the commercial spyware that pose significant counterintelligence or security risks to the United States Government or significant risks of improper use by a foreign government or foreign person.

Sec. 4. Reporting Requirements. (a) The head of each agency that has procured commercial spyware, upon completing the review described in section 2(h) of this order, shall submit to the APNSA a report describing the review's findings. If the review identifies any existing operational use of commercial spyware, as defined in this order, the agency report shall include:

(i) a description of such existing operational use;

(ii) a determination of whether the commercial spyware poses significant counterintelligence or security risks to the United States

Government or significant risks of improper use by a foreign government or foreign person, along with key elements of the underlying analysis, pursuant to section 2(a) of this order; and

(iii) in the event the agency determines that the commercial spyware poses significant risks pursuant to section 2(a) of this order, what steps have been taken to terminate its operational use.

(b) Within 45 days of an agency's procurement of any commercial spyware for any use described in section 2(l) of this order except for use in a criminal investigation arising out of the criminal sale or use of the spyware, the head of the agency shall notify the APNSA of such procurement and shall include in the notification a description of the purpose and authorized uses of the commercial spyware.

(c) Within 6 months of the date of this order, the head of each agency that has made operational use of commercial spyware or has procured commercial spyware for operational

use shall submit to the APNSA a report on the actions that the agency has taken to implement this order, including the internal controls and oversight procedures the agency has developed pursuant to section 2(i) of this order.

(d) Within 1 year of the date of this order, and on an annual basis thereafter, the head of each agency that has procured commercial spyware for operational use shall provide the APNSA a report that identifies:

(i) any existing operational use of commercial spyware and the reasons why it does not pose significant counterintelligence or security risks to the United States Government or significant risks of improper use by a foreign government or foreign person, pursuant to section 2(a) of this order;

(ii) any operational use of commercial spyware that was terminated during the preceding year because it was determined to pose significant risks pursuant to section 2(a) of this order, the circumstances

under which this determination was made, and the steps taken to terminate such use; and

(iii) any purchases made of commercial spyware, and whether they were made for operational use, during the preceding year.

Sec. 5. Definitions. For purposes of this order:

(a) The term "agency" means any authority of the United States that is an "agency" under 44 U.S.C. 3502(1), other than those considered to be independent regulatory agencies, as defined in 44 U.S.C. 3502(5).

(b) The term "commercial spyware" means any end-to-end software suite that is furnished for commercial purposes, either directly or indirectly through a third party or subsidiary, that provides the user of the software suite the capability to gain remote access to a computer, without the consent of the user, administrator, or owner of the computer, in order to:

(i) access, collect, exploit,

extract, intercept, retrieve, or transmit content, including information stored on or transmitted through a computer connected to the Internet;

(ii) record the computer's audio calls or video calls or use the computer to record audio or video; or

(iii) track the location of the computer.

(c) The term "computer" shall have the same meaning as it has in 18 U.S.C. 1030(e)(1).

(d) The term "entity" means a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization.

(e) The term "foreign entity" means an entity that is not a United States entity.

(f) The term "foreign government" means any national, state, provincial, or other governing authority, any political party, or any official of any governing authority or political party, in each case of a country other than the United States.

(g) The term "foreign person" means a person that is not a United States person.

(h) The term "furnish," when used in connection with commercial spyware, means to develop, maintain, own, operate, manufacture, market, sell, resell, broker, lease, license, repackage, rebrand, or otherwise make available commercial spyware.

(i) The term "operational use" means use to gain remote access to a computer, without the consent of the user, administrator, or owner of the computer, in order to:

(i) access, collect, exploit, extract, intercept, retrieve, or transmit the computer's content, including information stored on or transmitted through a computer connected to the Internet;

(ii) record the computer's audio calls or video calls or use the computer to otherwise record audio or video; or

(iii) track the location of the

computer.

The term "operational use" does not include those uses described in section 2(l) of this order.

(j) The term "person" means an individual or entity.

(k) The term "relevant official," for purposes of sections 2(f) and 2(m) of this order, refers to any of the following: the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the DNI, the Director of the Central Intelligence Agency, or the Director of the National Security Agency. The Attorney General's obligation under section 2(f) of this order and authority under section 2(m) of this order may be delegated only to the Deputy Attorney General.

(l) The term "remote access," when used in connection with commercial spyware, means access to a computer, the computer's content, or the computer's components by using an external network (e.g., the Internet) when the computer is not in the physical possession of the actor

seeking access to that computer.

(m) The term "United States entity" means any entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches).

(n) The term "United States person" shall have the same meaning as it has in Executive Order 12333 of December 4, 1981 (United States Intelligence Activities), as amended.

(o) The term "United States Government personnel" means all United States Government employees as defined by 5 U.S.C. 2105.

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) Nothing in this order shall be construed to limit the use of any remedies available to the head of an agency or any other official of the United States Government.

(c) This order shall be implemented consistent with applicable law, including section 6318 of the NDAA FY 2023, as well as applicable procurement laws, and subject to the availability of appropriations.

(d) 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,
March 27, 2023.