Editorial Notes

CODIFICATION

Section was formerly classified to section 442a of this title prior to editorial reclassification and renumbering as this section.

AMENDMENTS

2010—Subsec. (a). Pub. L. 111–259, § 409(1), struck out par. (1) designation before ''In'' and par. (2) which read as follows: ''The Director shall carry out the process through the Office of the National Counterintelligence Executive.''

Subsec. (b). Pub. L. 111–259, § 347(e), struck out par. (1) designation before ''The Director'' and par. (2) which read as follows: ''Not later than October 15 of each year, the Director shall certify to the congressional intelligence committees that the review required under paragraph (1) has been conducted in all elements of the intelligence community during the preceding fiscal year.''

Subsec. (c). Pub. L. 111–259, § 409(2), struck out par. (1) designation before ''The Director'' and par. (2) which read as follows: ''The Director shall carry out paragraph (1) through the Office of the National Counterintelligence Executive.''

2004—Subsec. (a)(1). Pub. L. 108–458, § 1071(a)(1)(NN), substituted ''Director of National Intelligence'' for ''Director of Central Intelligence''.

Subsec. (b)(1). Pub. L. 108–458, § 1071(a)(1)(OO), substituted ''Director of National Intelligence'' for ''Director of Central Intelligence''.

Subsec. (c)(1). Pub. L. 108–458, § 1071(a)(1)(PP), substituted ''Director of National Intelligence'' for ''Director of Central Intelligence''.

Subsec. (d). Pub. L. 108–458, § 1071(a)(1)(QQ), substituted ''Director of National Intelligence'' for ''Director of Central Intelligence''.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 2004 AMENDMENT

For Determination by President that amendment by Pub. L. 108–458 take effect on Apr. 21, 2005, see Memorandum of President of the United States, Apr. 21, 2005, 70 F.R. 23925, set out as a note under section 3001 of this title.

Amendment by Pub. L. 108–458 effective not later than six months after Dec. 17, 2004, except as otherwise expressly provided, see section 1097(a) of Pub. L. 108–458, set out in an Effective Date of 2004 Amendment; Transition Provisions note under section 3001 of this title.

§ 3232a. Measures to mitigate counterintelligence threats from proliferation and use of foreign commercial spyware

(a) Definitions

In this section:

(1) Appropriate congressional committees

The term ''appropriate congressional committees'' means—

(A) the Select Committee on Intelligence, the Committee on Foreign Relations, the Committee on Armed Services, the Committee on Banking, Housing, and Urban Affairs, the Committee on the Judiciary, the Committee on Appropriations, and the Committee on Homeland Security and Governmental Affairs of the Senate; and

(B) the Permanent Select Committee on Intelligence, the Committee on Foreign Affairs, the Committee on Armed Services, the Committee on Financial Services, the Committee on the Judiciary, the Committee on Appropriations, the Committee on Homeland Security, and the Committee on Oversight and Reform of the House of Representatives.

(2) Covered entity

The term ''covered entity'' means any foreign company that either directly or indirectly develops, maintains, owns, operates, brokers, markets, sells, leases, licenses, or otherwise makes available spyware.

(3) Foreign commercial spyware

The term ''foreign commercial spyware'' means spyware that is developed (solely or in partnership with a foreign company), maintained, sold, leased, licensed, marketed, sourced (in whole or in part), or otherwise provided, either directly or indirectly, by a foreign company.

(4) Foreign company

The term ''foreign company'' means a company that is incorporated or domiciled outside of the United States, including any subsidiaries or affiliates wherever such subsidiaries or affiliates are domiciled or incorporated.

(5) Spyware

The term ''spyware'' means a tool or set of tools that operate as an end-to-end system of software to provide an unauthorized user remote access to information stored on or transiting through an electronic device connected to the Internet and not owned or operated by the unauthorized user, including end-to-end systems that—

(A) allow an unauthorized user to remotely infect electronic devices with malicious software, including without any action required by the user of the device;

(B) can record telecommunications or other audio captured on a device not owned by the unauthorized user;

(C) undertake geolocation, collect cell site location information, or otherwise track the location of a device or person using the internal sensors of an electronic device not owned by the unauthorized user;

(D) allow an unauthorized user access to and the ability to retrieve information on the electronic device, including text messages, files, e-mails, transcripts of chats, contacts, photos, and browsing history; or

(E) any additional criteria described in publicly available documents published by the Director of National Intelligence, such as whether the end-to-end system is used outside the context of a codified lawful intercept system.

(b) Annual assessments of counterintelligence threats

(1) Requirement

Not later than 90 days after December 23, 2022, and annually thereafter, the Director of National Intelligence, in coordination with the Director of the Central Intelligence Agency, the Director of the National Security Agency, and the Director of the Federal Bureau of Investigation, shall submit to the appropriate congressional committees a report with an accompanying classified annex con-

taining an assessment of the counterintelligence threats and other risks to the national security of the United States posed by the proliferation of foreign commercial spyware. The assessment shall incorporate all credible data, including open-source information.

(2) Elements

Each report under paragraph (1) shall include the following, if known:

(A) A list of the most significant covered entities.

(B) A description of the foreign commercial spyware marketed by the covered entities identified under subparagraph (A) and an assessment by the intelligence community of the foreign commercial spyware.

(C) An assessment of the counterintelligence risk to the intelligence community or personnel of the intelligence community posed by foreign commercial spyware.

(D) For each covered entity identified in subparagraph (A), details of any subsidiaries, resellers, or other agents acting on behalf of the covered entity.

(E) Details of where each covered entity identified under subparagraphs (A) and (D) is domiciled.

(F) A description of how each covered entity identified under subparagraphs (A) and (D) is financed, where the covered entity acquired its capital, and the organizations and individuals having substantial investments or other equities in the covered entity.

(G) An assessment by the intelligence community of any relationship between each covered entity identified in subparagraphs (A) and (D) and any foreign government, including any export controls and processes to which the covered entity is subject.

(H) A list of the foreign customers of each covered entity identified in subparagraphs (A) and (D), including the understanding by the intelligence community of the organizations and end-users within any foreign government.

(I) With respect to each foreign customer identified under subparagraph (H), an assessment by the intelligence community regarding how the foreign customer is using the spyware, including whether the foreign customer has targeted personnel of the intelligence community.

(J) With respect to the first report required under paragraph (1), a mitigation plan to reduce the exposure of personnel of the intelligence community to foreign commercial spyware.

(K) With respect to each report following the first report required under paragraph (1), details of steps taken by the intelligence community since the previous report to implement measures to reduce the exposure of personnel of the intelligence community to foreign commercial spyware.

(3) Classified annex

In submitting the report under paragraph (1), the Director shall also include an accompanying but separate classified annex, providing a watchlist of companies selling, leasing, or otherwise providing foreign commercial spyware that the Director determines are engaged in activities that pose a counterintelligence risk to personnel of the intelligence community.

(4) Form

Each report under paragraph (1) shall be submitted in classified form.

(5) Dissemination

The Director of National Intelligence shall separately distribute each report under paragraph (1) and each annex under paragraph (3) to the President, the heads of all elements of the intelligence community, the Secretary of State, the Attorney General, the Secretary of Commerce, the Secretary of Homeland Security, the National Cyber Director, and the heads of any other departments or agencies the Director of National Intelligence determines appropriate.

(c) Authority to prohibit purchase or use by intelligence community

(1) Foreign commercial spyware

(A) In general

The Director of National Intelligence may prohibit any element of the intelligence community from procuring, leasing, or otherwise acquiring on the commercial market, or extending or renewing a contract to procure, lease, or otherwise acquire, foreign commercial spyware.

(B) Considerations

In determining whether and how to exercise the authority under subparagraph (A), the Director of National Intelligence shall consider—

(i) the assessment of the intelligence community of the counterintelligence threats or other risks to the United States posed by foreign commercial spyware;

(ii) the assessment of the intelligence community of whether the foreign commercial spyware has been used to target United States Government personnel;

(iii) whether the original owner or developer retains any of the physical property or intellectual property associated with the foreign commercial spyware;

(iv) whether the original owner or developer has verifiably destroyed all copies of the data collected by or associated with the foreign commercial spyware;

(v) whether the personnel of the original owner or developer retain any access to data collected by or associated with the foreign commercial spyware;

(vi) whether the use of the foreign commercial spyware requires the user to connect to an information system of the original owner or developer or information system of a foreign government; and

(vii) whether the foreign commercial spyware poses a counterintelligence risk to the United States or any other threat to the national security of the United States.

(2) Company that has acquired foreign commercial spyware

(A) Authority

The Director of National Intelligence may prohibit any element of the intelligence

community from entering into any contract or other agreement for any purpose with a company that has acquired, in whole or in part, any foreign commercial spyware.

(B) Considerations

In considering whether and how to exercise the authority under subparagraph (A), the Director of National Intelligence shall consider—

(i) whether the original owner or developer of the foreign commercial spyware retains any of the physical property or intellectual property associated with the spyware;

(ii) whether the original owner or developer of the foreign commercial spyware has verifiably destroyed all data, and any copies thereof, collected by or associated with the spyware;

(iii) whether the personnel of the original owner or developer of the foreign commercial spyware retain any access to data collected by or associated with the foreign commercial spyware;

(iv) whether the use of the foreign commercial spyware requires the user to connect to an information system of the original owner or developer or information system of a foreign government; and

(v) whether the foreign commercial spyware poses a counterintelligence risk to the United States or any other threat to the national security of the United States.

(3) Notifications of prohibition

Not later than 30 days after the date on which the Director of National Intelligence exercises the authority to issue a prohibition under subsection (c), the Director of National Intelligence shall notify the congressional intelligence committees of such exercise of authority. Such notice shall include—

(A) a description of the circumstances under which the prohibition was issued;

(B) an identification of the company or product covered by the prohibition;

(C) any information that contributed to the decision of the Director of National Intelligence to exercise the authority, including any information relating to counterintelligence or other risks to the national security of the United States posed by the company or product, as assessed by the intelligence community; and

(D) an identification of each element of the intelligence community to which the prohibition has been applied.

(4) Waiver authority

(A) In general

The head of an element of the intelligence community may request from the Director of National Intelligence the waiver of a prohibition made under paragraph (1) or (2).

(B) Director of National Intelligence determination

The Director of National Intelligence, upon receiving the waiver request in subparagraph (A), may issue a waiver for a period not to exceed one year in response to the request from the head of an element of the intelligence community if such waiver is in the national security interest of the United States.

(C) Notice

Not later than 30 days after approving a waiver request pursuant to subparagraph (B), the Director of National Intelligence shall submit to the congressional intelligence committees, the Subcommittee on Defense of the Committee on Appropriations of the Senate, and the Subcommittee on Defense of the Committee on Appropriations of the House of Representatives a written notification. The notification shall include—

(i) an identification of the head of the element of the intelligence community that requested the waiver;

(ii) the details of the waiver request, including the national security interests of the United States;

(iii) the rationale and basis for the determination that the waiver is in the national security interests of the United States;

(iv) the considerations that informed the ultimate determination of the Director of National Intelligence to issue the waiver; and

(v) and any other considerations contributing to the determination, made by the Director of National Intelligence.

(D) Waiver termination

The Director of National Intelligence may revoke a previously granted waiver at any time. Upon revocation of a waiver, the Director of National Intelligence shall submit a written notification to the congressional intelligence committees, the Subcommittee on Defense of the Committee on Appropriations of the Senate, and the Subcommittee on Defense of the Committee on Appropriations of the House of Representatives not later than 30 days after making a revocation determination.

(5) Termination of prohibition

The Director of National Intelligence may terminate a prohibition made under paragraph (1) or (2) at any time. Upon termination of a prohibition, the Director of National Intelligence shall submit a notification of the termination to the congressional intelligence committees, the Subcommittee on Defense of the Committee on Appropriations of the Senate, and the Subcommittee on Defense of the Committee on Appropriations of the House of Representatives not later than 30 days after terminating a prohibition, detailing the basis for the termination, including any United States national security interests that may be affected by such termination.

(July 26, 1947, ch. 343, title XI, § 1102A, as added Pub. L. 117–263, div. F, title LXIII, § 6318(c), Dec. 23, 2022, 136 Stat. 3515; amended Pub. L. 118–31, div. G, title IX, § 7901(a)(4), Dec. 22, 2023, 137 Stat. 1106; Pub. L. 118–159, div. F, title LXIX, § 6902(a)(3), Dec. 23, 2024, 138 Stat. 2517.)

Editorial Notes

AMENDMENTS

2024—Subsec. (c)(1)(B)(ii). Pub. L. 118–159 substituted semicolon for period at end.

2023—Subsec. (b)(3). Pub. L. 118–31, § 7901(a)(4)(A), substituted ''paragraph (1)'' for ''subsection (2)''.

Subsec. (c)(4)(C)(iv). Pub. L. 118–31, § 7901(a)(4)(B), substituted ''waiver'' for ''wavier''.

Statutory Notes and Related Subsidiaries

CHANGE OF NAME

Committee on Oversight and Reform of House of Representatives changed to Committee on Oversight and Accountability of House of Representatives by House Resolution No. 5, One Hundred Eighteenth Congress, Jan. 9, 2023.

RULE OF CONSTRUCTION—NO ENHANCED AUTHORITIES

Pub. L. 117–263, div. F, title LXIII, § 6318(e), Dec. 23, 2022, 136 Stat. 3521, provided that: ''Nothing in this section [enacting this section, amending section 3383 of this title, and enacting provisions set out as notes under this section] or an amendment made by this section shall be construed as enhancing, or otherwise changing, the authorities of the intelligence community to target, collect, process, or disseminate information regarding United States Government personnel.''

[For definition of ''intelligence community'' as used in section 6318(e) of Pub. L. 117–263, set out above, see section 6002 of Pub. L. 117–263, set out as a note under section 3003 of this title.]

STATEMENT OF POLICY

Pub. L. 117–263, div. F, title LXIII, § 6318(b), Dec. 23, 2022, 136 Stat. 3515, provided that: ''It shall be the policy of the United States to act decisively against counterintelligence threats posed by foreign commercial spyware, as well as the individuals who lead entities selling foreign commercial spyware and who are reasonably believed to be involved, have been involved, or pose a significant risk to being or becoming involved, in activities contrary to the national security or foreign policy interests of the United States.''

[For definition of ''foreign commercial spyware'' as used in section 6318(b) of Pub. L. 117–263, set out above, see section 6318(a) of Pub. L. 117–263, set out below.]

PROTECTION OF COVERED DEVICES

Pub. L. 117–263, div. F, title LXIII, § 6318(d)(1)–(3), Dec. 23, 2022, 136 Stat. 3520, provided that:

''(1) REQUIREMENT.—Not later than 120 days after the date of the enactment of this Act [Dec. 23, 2022], the Director of National Intelligence shall—

''(A) issue standards, guidance, best practices, and policies for elements of the intelligence community to protect covered devices from being compromised by foreign commercial spyware;

''(B) survey elements of the intelligence community regarding the processes used by the elements to routinely monitor covered devices for indicators of compromise associated with foreign commercial spyware; and

''(C) submit to the congressional intelligence committees a report on the sufficiency of the measures in place to routinely monitor covered devices for indicators of compromise associated with foreign commercial spyware.

''(2) FORM.—The report under paragraph (1)(C) may be submitted in classified form.

''(3) COUNTERINTELLIGENCE NOTIFICATIONS.—Not later than 30 days after the date on which an element of the intelligence community becomes aware that a covered device was targeted or compromised by foreign commercial spyware, the Director of National Intelligence, in coordination with the Director of the Federal Bureau of Investigation, shall notify the congressional intelligence committees, the Subcommittee on Defense of the Committee on Appropriations of the Senate, and the Subcommittee on Defense of the Committee on Appropriations of the House of Representatives of such determination, including—

''(A) the component of the element and the location of the personnel whose covered device was targeted or compromised;

''(B) the number of covered devices compromised or targeted;

''(C) an assessment by the intelligence community of the damage to national security of the United States resulting from any loss of data or sensitive information;

''(D) an assessment by the intelligence community of any foreign government, or foreign organization or entity, and, to the extent possible, the foreign individuals, who directed and benefitted from any information acquired from the targeting or compromise; and

''(E) as appropriate, an assessment by the intelligence community of the capacity and will of such governments or individuals to continue targeting personnel of the United States Government.''

[For definitions of ''intelligence community'' and ''congressional intelligence committees'' as used in section 6318(d)(1)–(3) of Pub. L. 117–263, set out above, see section 6002 of Pub. L. 117–263, set out as a note under section 3003 of this title.]

[For definitions of ''covered device'' and ''foreign commercial spyware'' as used in section 6318(d)(1)–(3) of Pub. L. 117–263, set out above, see section 6318(a) of Pub. L. 117–263, set out below.]

DEFINITIONS

Pub. L. 117–263, div. F, title LXIII, § 6318(a), Dec. 23, 2022, 136 Stat. 3515, provided that: ''In this section:

''(1) COVERED DEVICE.—The term 'covered device' means any electronic mobile device including smartphones, tablet computing devices, or laptop computing devices, that is issued by an element of the intelligence community for official use.

''(2) FOREIGN COMMERCIAL SPYWARE; FOREIGN COMPANY; SPYWARE.—The terms 'foreign commercial spyware', 'foreign company', and 'spyware' have the meanings given those terms in section 1102A of the National Security Act of 1947 (50 U.S.C. 3231 et seq. [probably means 50 U.S.C. 3232a]), as added by this section.''

[For definition of ''intelligence community'' as used in section 6318(a) of Pub. L. 117–263, set out above, see section 6002 of Pub. L. 117–263, set out as a note under section 3003 of this title.]

Executive Documents

EX. ORD. NO. 14093. PROHIBITION ON USE BY THE UNITED STATES GOVERNMENT OF COMMERCIAL SPYWARE THAT POSES RISKS TO NATIONAL SECURITY

Ex. Ord. No. 14093, Mar. 27, 2023, 88 F.R. 18957, provided:

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) [enacting this section and provisions set out as notes above] and section 5502 of the National Defense Authorization Act for Fiscal Year 2022 (NDAA FY 2022) (Public Law 117–81) [22 U.S.C. 2679e].

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 sub-

section (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 [Mar. 27, 2023], 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. 3232a(b)], 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 CFR 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) [50 U.S.C. 3001 note], 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.

J.R. BIDEN, JR.

§ 3233. Misuse of the Office of the Director of National Intelligence name, initials, or seal

(a) Prohibited acts

No person may, except with the written permission of the Director of National Intelligence, or a designee of the Director, knowingly use the