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

words ''Office of the Director of National Intelligence'', the initials ''ODNI'', the seal of the Office of the Director of National Intelligence, or any colorable imitation of such words, initials, or seal in connection with any merchandise, impersonation, solicitation, or commercial activity in a manner reasonably calculated to convey the impression that such use is approved, endorsed, or authorized by the Director of National Intelligence.

(b) Injunction

Whenever it appears to the Attorney General that any person is engaged or is about to engage in an act or practice which constitutes or will constitute conduct prohibited by subsection (a), the Attorney General may initiate a civil proceeding in a district court of the United States to enjoin such act or practice. Such court shall proceed as soon as practicable to the hearing and determination of such action and may, at any time before final determination, enter such restraining orders or prohibitions, or take such other action as is warranted, to prevent injury to the United States or to any person or class of persons for whose protection the action is brought.

(July 26, 1947, ch. 343, title XI, § 1103, as added Pub. L. 111–259, title IV, § 413(a), Oct. 7, 2010, 124 Stat. 2726.)

Editorial Notes

CODIFICATION

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

§ 3234. Prohibited personnel practices in the intelligence community

(a) Definitions

In this section:

(1) Agency

The term ''agency'' means an executive department or independent establishment, as defined under sections 101 and 104 of title 5, that contains an intelligence community element, except the Federal Bureau of Investigation.

(2) Covered intelligence community element

The term ''covered intelligence community element''—

(A) means—

(i) the Central Intelligence Agency, the Defense Intelligence Agency, the National Geospatial-Intelligence Agency, the National Security Agency, the Office of the Director of National Intelligence, and the National Reconnaissance Office; and

(ii) any executive agency or unit thereof determined by the President under section 2302(a)(2)(C)(ii) of title 5 to have as its principal function the conduct of foreign intelligence or counterintelligence activities; and

(B) does not include the Federal Bureau of Investigation.

(3) Personnel action

The term ''personnel action'' means, with respect to an employee in a position in a covered intelligence community element (other than a position excepted from the competitive service due to its confidential, policy-determining, policymaking, or policy-advocating character) or a contractor employee—

(A) an appointment;

(B) a promotion;

(C) a disciplinary or corrective action;

(D) a detail, transfer, or reassignment;

(E) a demotion, suspension, or termination;

(F) a reinstatement or restoration;

(G) a performance evaluation;

(H) a decision concerning pay, benefits, or awards;

(I) a decision concerning education or training if such education or training may reasonably be expected to lead to an appointment, promotion, or performance evaluation; or

(J) any other significant change in duties, responsibilities, or working conditions.

(4) Contractor employee

The term ''contractor employee'' means an employee of a contractor, subcontractor, grantee, subgrantee, or personal services contractor, of a covered intelligence community element.

(b) Agency employees

Any employee of a covered intelligence community element or an agency who has authority to take, direct others to take, recommend, or approve any personnel action, shall not, with respect to such authority, take or fail to take, or threaten to take or fail to take, a personnel action with respect to any employee of a covered intelligence community element as a reprisal for—

(1) any lawful disclosure of information by the employee to the Director of National Intelligence (or an employee designated by the Director of National Intelligence for such purpose), the Inspector General of the Intelligence Community, a supervisor in the employee's direct chain of command, or a supervisor of the employing agency with responsibility for the subject matter of the disclosure, up to and including the head of the employing agency (or an employee designated by the head of that agency for such purpose), the appropriate inspector general of the employing agency or covered intelligence community element, a congressional intelligence committee, or a member of a congressional intelligence committee, which the employee reasonably believes evidences—

(A) a violation of any Federal law, rule, or regulation; or

(B) mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety;

(2) any lawful disclosure that complies with—

(A) subsections (b)(1), (e), and (h) of section 416 of title 5;

(B) subparagraphs (A), (D), and (H) of section 3517(d)(5) of this title; or

(C) subparagraphs (A), (D), and (I) of section 3033(k)(5) of this title; or