

SEC. 1018. CLARIFYING THE DEFAULT STATUTE OF LIMITATIONS.

(a) Correcting Corner Post, Inc. v. Board of Governors.—[Section 2401\(a\) of title 28](#), United States Code, is amended by striking "right of action first accrues" and inserting "last act or omission of the United States giving rise to the claim".

(b) Applicability.—This section and the amendment made by this section shall apply to any civil action pending on, or commenced on or after, the date of enactment of this Act, but shall not be construed to reopen any final judgment entered before the date of enactment of this Act.

Subtitle B—Reforming Government Surveillance

SEC. 1021. DEFINITIONS AND CONFORMING AMENDMENTS.

(a) Definitions relating to the Foreign Intelligence Surveillance Act of 1978.—

(1) In general.—Section 101 of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1801](#)) is amended by adding at the end the following:

"(q) The term 'Foreign Intelligence Surveillance Court' means the court established under section 103(a).

"(r) The terms 'Foreign Intelligence Surveillance Court of Review' and 'Court of Review' mean the court established under section 103(b).

"(s) The term 'appropriate committees of Congress' means—

"(1) the congressional intelligence committees (as defined in section 3 of the National Security Act of 1947 ([50 U.S.C. 3003](#)));

"(2) the Committee on the Judiciary of the Senate; and

"(3) the Committee on the Judiciary of the House of Representatives.".

(2) Title VII.—Section 701(b) of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1881](#)) is amended by adding at the end the following:

"(6) Covered person.—The term 'covered person' means, with respect to a query, a communication, an acquisition, or creation of information, a person who is—

"(A) a United States person; or

"(B) a person known or believed to be located in the United States—

"(i) at the time of the applicable query; or

"(ii) at the time of the acquisition, communication, or creation of the information subject to the applicable query.".

(b) Terms used in this subtitle.—In this subtitle—

(1) the terms "appropriate committees of Congress", "Foreign Intelligence Surveillance Court", and "Foreign Intelligence Surveillance Court of Review" have the meanings given such

terms in section 101 of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1801](#)), as amended by subsection (a)(1); and

(2) the term "covered person" has the meaning given such term in section 701 of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1881](#)), as amended by subsection (a)(2).

(c) Conforming amendments.—The Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1801 et seq.](#)) is amended—

(1) in section 102(a)(3) ([50 U.S.C. 1802\(a\)\(3\)](#)), by striking "the court established under section 103(a)" and inserting "the Foreign Intelligence Surveillance Court";

(2) in section 103 ([50 U.S.C. 1803](#))—

(A) in subsection (a)—

(i) in paragraph (2)(A), by striking "The court established under this subsection" and inserting "The Foreign Intelligence Surveillance Court"; and

(ii) by striking "the court established under this subsection" each place it appears and inserting "the Foreign Intelligence Surveillance Court";

(B) in subsection (g)—

(i) in paragraph (2)—

(I) in subparagraph (A), by striking "the court established pursuant to subsection (a)" and inserting "the Foreign Intelligence Surveillance Court"; and

(II) in subparagraph (B), by striking "the court of review established pursuant to subsection (b)" and inserting "the Foreign Intelligence Surveillance Court of Review"; and

(ii) in paragraph (1), by striking "The courts established pursuant to subsections (a) and (b)" and inserting "The Foreign Intelligence Surveillance Court and the Foreign Intelligence Surveillance Court of Review";

(C) in subsection (h), by striking "a court established under this section" and inserting "the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review";

(D) in subsection (i)—

(i) in paragraph (1), by striking "the courts established under subsections (a) and (b)" and inserting "the Foreign Intelligence Surveillance Court and the Foreign Intelligence Surveillance Court of Review";

(ii) in paragraph (3)(B), in the 1st sentence, by striking "the courts" and inserting "the Foreign Intelligence Surveillance Court and the Foreign Intelligence Surveillance Court of Review";

(iii) in paragraph (5), by striking "the court" and inserting "the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review, as the case may be,";

(iv) in paragraph (6), by striking "the court" each place it appears and inserting "the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review";

(v) by striking "a court established under subsection (a) or (b)" each place it appears and inserting "the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review"; and

(vi) by striking "A court established under subsection (a) or (b)" each place it appears and inserting "The Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review";

(E) in subsection (j)—

(i) by striking "a court established under subsection (a)" and inserting "the Foreign Intelligence Surveillance Court"; and

(ii) by striking "the court determines" and inserting "the Foreign Intelligence Surveillance Court determines";

(F) by striking "the court established under subsection (a)" each place it appears and inserting "the Foreign Intelligence Surveillance Court"; and

(G) by striking "the court established under subsection (b)" each place it appears and inserting "the Foreign Intelligence Surveillance Court of Review";

(3) in section 105(c)(3) ([50 U.S.C. 1805\(c\)\(3\)](#)), by striking "the court" each place it appears and inserting "the Foreign Intelligence Surveillance Court";

(4) in section 401(1) ([50 U.S.C. 1841\(1\)](#)), by striking "and 'State'" and inserting "'State', 'Foreign Intelligence Surveillance Court', and 'Foreign Intelligence Surveillance Court of Review'";

(5) in section 402 ([50 U.S.C. 1842](#))—

(A) in subsection (b)(1), by striking "the court established by section 103(a) of this Act" and inserting "the Foreign Intelligence Surveillance Court"; and

(B) in subsection (h)(2), by striking "the court established under section 103(a)" and inserting "the Foreign Intelligence Surveillance Court";

(6) in section 502(b)(1)(A), by striking "the court established by section 103(a) of this Act" and inserting "the Foreign Intelligence Surveillance Court (as defined by section 101)";

(7) in section 801 ([50 U.S.C. 1885](#))—

(A) in paragraph (8)(B)(i), by striking "the court established under section 103(a)" and inserting "the Foreign Intelligence Surveillance Court"; and

(B) by adding at the end the following:

"(10) Foreign Intelligence Surveillance Court.—The term 'Foreign Intelligence Surveillance Court' means the court established under section 103(a)."; and

(8) in section 802(a)(1) ([50 U.S.C. 1885a\(a\)\(1\)](#)), by striking "the court established under section 103(a)" and inserting "the Foreign Intelligence Surveillance Court".

SEC. 1022. SECTION 702 REFORM.

(a) Protections related to warrantless queries.—Section 702(f) of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1881a\(f\)](#)) is amended—

(1) in paragraph (1)(A), by inserting "and the limitations and requirements in this subsection" after "Constitution of the United States";

(2) in paragraph (5)—

(A) in subparagraph (B), by striking "means" and all that follows through the period and inserting the following: "means the use of 1 or more terms, whether conducted through manual or automated means, to retrieve any information acquired under this section, including retrieval from a subset of such information, whether that subset was created by retrieval through a query or other means.";

(B) by redesignating subparagraph (B) as subparagraph (D); and

(C) by inserting after subparagraph (A) the following:

"(B) The term 'covered information' means—

"(i) communications content; and

"(ii) information, the compelled disclosure of which would require a probable cause warrant if sought for law enforcement purposes inside the United States.

"(C) The term 'covered query' means a query that is conducted—

"(i) using a term associated with 1 or more covered persons; or

"(ii) for a significant purpose of retrieving information of or concerning 1 or more covered persons."; and

(3) by amending paragraph (6) to read as follows:

"(6) Prohibition on warrantless queries for the communications and other information of covered persons located in the United States.—

"(A) In general.—Except as provided in subparagraphs (B) and (C), no officer or employee of the Federal Government may access covered information returned in response to a covered query.

"(B) Exceptions for concurrent authorization, consent, emergency situations, and certain defensive cybersecurity queries.—Subparagraph (A) shall not apply if—

"(i) the covered person to whom the covered query relates is the subject of an order or emergency authorization authorizing electronic surveillance or physical search under section 105 or 304 of this Act, or a warrant issued pursuant to the Federal Rules of Criminal Procedure by a court of competent jurisdiction, if—

"(I) such order, authorization, or warrant covers the period of the covered query; and

"(II) the covered query is conducted and covered information is accessed in compliance with all use, dissemination, querying, retention, and other minimization limitations required by the order, authorization, or warrant;

"(ii) (I) the officer or employee accessing the covered information has a reasonable belief that—

"(aa) an emergency exists involving an imminent threat of death or serious bodily harm; and

"(bb) in order to prevent or mitigate the threat described in item (aa), the covered information must be accessed before authorization described in clause (i) can, with due diligence, be obtained; and

"(II) not later than 14 days after the covered information is accessed, a description of the circumstances justifying the accessing of the covered information is provided to the Foreign Intelligence Surveillance Court and the appropriate committees of Congress;

"(iii) the covered person to whom the covered query relates or, if such person is incapable of providing consent, a third party legally authorized to consent on behalf of such person, has provided consent for the access on a case-by-case basis; or

"(iv) (I) the covered information is accessed and used for defensive cybersecurity purposes, including the protection of a covered person from cybersecurity attack;

"(II) other than for such defensive cybersecurity purposes, no covered information is accessed or reviewed; and

"(III) not later than 14 days after the covered information is accessed, a description of the circumstances justifying the accessing of the covered information is provided to the Foreign Intelligence Surveillance Court and the appropriate committees of Congress.

"(C) Matters relating to emergency queries.—

"(i) Treatment of denials.—If covered information is accessed pursuant to an emergency authorization described in subparagraph (B)(i) and the subsequent application to authorize electronic surveillance, a physical search, or an acquisition pursuant to section 105(e) or section 304(e) of this Act is denied, or in any other case in which covered information is accessed in violation of this paragraph—

"(I) no covered information accessed, or information or evidence derived from such access may be used, received in evidence, or otherwise disseminated in any investigation, trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof; and

"(II) no covered information accessed may subsequently be used or disclosed in any other manner without the consent of such person, except if the Attorney General personally approves the use or disclosure of such information in order to prevent the death of or serious bodily harm to any person and not later than 14 days after such approval, a description of the circumstances justifying the approval is provided to the Foreign Intelligence Surveillance Court and the appropriate committees of Congress.

"(ii) Assessment of compliance.—Not less frequently than once each year, the Attorney General shall assess compliance with the requirements under clause (i).

"(D) Foreign intelligence purpose required for queries.—

"(i) In general.—Except as provided in clause (ii), no officer or employee of the Federal Government may conduct a query unless the query is—

"(I) reasonably likely to retrieve foreign intelligence information; and

"(II) made with a significant foreign intelligence purpose.

"(ii) Exceptions.—An officer or employee of the Federal Government is permitted to conduct a query if an exception described in clauses (i) and (ii) of paragraph (2)(B) applies.

"(E) Documentation.—No officer or employee of the Federal Government may conduct a query, or access covered information returned in response to a covered query, unless an electronic record is created that includes—

"(i) for each query—

"(I) each term used for the conduct of the query;

"(II) the date of the query;

"(III) the identifier of the officer or employee who conducted the query; and

"(IV) a statement of facts justifying that the query is reasonably likely to retrieve foreign intelligence information and the significant foreign intelligence purpose for the query or, if an exception under subparagraph (D)(ii) applies, a description of the basis for such exception; and

"(ii) for each access—

"(I) the date of the access;

"(II) the identifier of the officer or employee who did the particular access; and

"(III) a statement of facts showing that an access is authorized by an exception under subparagraph (B).

"(F) Query record system.—The head of each agency authorized to conduct a covered query shall ensure that a system, mechanism, or business practice is in place to maintain the records described in subparagraph (E), including ensuring that any queries or accesses to covered information returned in response to covered queries, that are conducted by automated means are attributed to the officer or employee who was the proximate cause of such query or access."

(b) Report on compliance with query record system requirement.—Not later than 90 days after the date of enactment of this Act, each head of a Federal agency described in section 702(f)(6)(F) of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1881a\(f\)\(6\)\(F\)](#)), as added by subsection (a), shall submit to the appropriate committees of Congress a report on the compliance of the Federal agency with the requirement of such section.

(c) Conforming amendments.—Section 702(f) of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1881a\(f\)](#)), as amended by subsection (a), is further amended—

(1) in the headings for subparagraph (B) of paragraph (1), subparagraph (A) of paragraph (2), and subparagraph (A) of paragraph (3), by striking "united states person" each place it appears and inserting "covered person";

(2) in paragraphs (1) through (5), by striking "United States person" each place it appears and inserting "covered person".

(d) Limitation on use of information obtained under section 702 relating to covered persons in criminal, civil, and administrative actions.—Paragraph (2) of section 706(a) of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1881e\(a\)](#)) is amended—

(1) in the paragraph heading, by striking "United States persons" and inserting "Covered persons"; and

(2) in subparagraph (A)—

(A) by striking "United States person" both places it appears and inserting "covered person";

(B) in the matter before clause (i), by striking "in any criminal proceeding" and inserting "in any criminal, civil, or administrative proceeding"; and

(C) in clause (ii), by striking "the criminal proceeding" both places it appears and inserting "the proceeding".

(e) Prohibition on reverse targeting of covered persons located in the United States.—Section 702 of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1881a](#)), as amended by this section, is further amended—

(1) in subsection (b)—

(A) by redesignating paragraph (6) as paragraph (7); and

(B) by inserting after paragraph (5) the following:

"(6) may not intentionally target a person reasonably believed to be located outside the United States if a significant purpose of such acquisition is to acquire the information of 1 or more particular, known covered persons, unless—

"(A) (i) there is a reasonable belief that an emergency exists involving an imminent threat of death or serious bodily harm to such covered persons;

"(ii) the information is sought for the purpose of assisting those covered persons; and

"(iii) not later than 14 days after the targeting, a description of the targeting is provided to the Foreign Intelligence Surveillance Court and the appropriate committees of Congress; or

"(B) the covered persons have provided consent to the targeting, or if such persons are incapable of providing consent, a third party legally authorized to consent on behalf of such covered person has provided consent;"

(2) in subsection (d)(1), by amending subparagraph (A) to read as follows:

"(A) ensure that—

"(i) any acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be non-United States persons located outside the United States; and

"(ii) except as provided in subsection (b)(6), it is not a significant purpose of an acquisition to acquire the information of 1 or more particular, known covered persons; and";

(3) in subsection (h)(2)(A)(i), by amending subclause (I) to read as follows:

"(I) ensure that—

"(aa) an acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be non-United States persons located outside the United States; and

"(bb) except as provided in subsection (b)(6), it is not a significant purpose of an acquisition to acquire the information of 1 or more particular, known covered persons; and"; and

(4) in subsection (j)(2)(B), by amending clause (i) to read as follows:

"(i) ensure that—

"(I) an acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be non-United States persons located outside the United States; and

"(II) except as provided in subsection (b)(6), it is not a significant purpose of an acquisition to acquire the information of 1 or more particular, known covered persons; and".

(f) Data retention limits for information collected under section 702.—Title VII of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1881 et seq.](#)) is amended by adding at the end the following:

"Sec. 710. Data retention limits.

"(a) Policy.—The Attorney General shall develop, and the heads of the elements of the intelligence community shall implement, procedures governing the retention of information collected pursuant to section 702.

"(b) Covered information.—For purposes of this section, 'covered information' includes—

"(1) any information or communication pertaining to a covered person, including an encrypted communication to or from such person, regardless of whether such communication is encrypted; and

"(2) any communication to or from a person, regardless of whether such communication is encrypted.

"(c) Requirements.—The procedures developed and implemented pursuant to subsection (a) shall ensure, with respect to information described in such subsection, that covered information shall be destroyed within 5 years of collection unless the Attorney General determines in writing that—

"(1) the information is the subject of a preservation obligation in pending administrative, civil, or criminal litigation, in which case the information shall be segregated, retained, and used solely for that purpose and shall be destroyed as soon as it is no longer required to be preserved for such litigation; or

"(2) the information is being used in a proceeding or investigation consistent with section 706(a).".

(g) Clerical amendment relating to data retention limits.—The table of contents for the Foreign Intelligence Surveillance Act of 1978 is amended by inserting after the item relating to section 709 the following:

"710. Data retention limits."

(h) Foreign Intelligence Surveillance Court supervision of demands for technical assistance from electronic communication service providers under section 702.—Section 702(i)(1) of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1881a\(i\)\(1\)](#)) is amended—

(1) by redesignating subparagraphs (A) and (B) as clauses (i) and (ii), respectively, and moving such clauses 2 ems to the right;

(2) in the matter before clause (i), as redesignated by paragraph (1), by striking "With respect to" and inserting the following:

"(A) In general.—Subject to subparagraph (B), in carrying out"; and

(3) by adding at the end the following:

"(B) Limitations.—Neither the Attorney General nor the Director of National Intelligence may direct technical assistance from an electronic communication service provider under subparagraph (A) without demonstrating that the assistance sought—

"(i) is necessary;

"(ii) is narrowly tailored to the surveillance at issue; and

"(iii) would not pose an undue burden on the electronic communication service provider or its customers who are not intended targets of the surveillance.

"(C) Compliance.—An electronic communication service provider is not obligated to comply with a directive to provide technical assistance under this paragraph unless—

"(i) such assistance is a manner or method that has been explicitly approved by the Court; and

"(ii) the Court issues an order, which has been delivered to the provider, explicitly describing the assistance to be furnished by the provider that has been approved by the Court."

(i) Prohibition on warrantless acquisition of domestic communications pursuant to section 702.—Section 702 of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1881a](#)) is amended—

(1) in subsection (b)(4), by striking "known at the time of the acquisition" and inserting "known or believed at the time of acquisition or communication";

(2) in subsection (d)(1)(B), by striking "known at the time of the acquisition" and inserting "known or believed at the time of acquisition or communication";

(3) in subsection (h)(2)(A)(i)(II), by striking "known at the time of the acquisition" and inserting "known or believed at the time of acquisition or communication"; and

(4) in subsection (j)(2)(B)(ii), by striking "known at the time of the acquisition" and inserting "known or believed at the time of acquisition or communication".

(j) Requirement of primary foreign intelligence purpose.—Section 702(h)(2)(A)(v) of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1881a\(h\)\(2\)\(A\)\(v\)](#)) is amended by striking "a significant" and inserting "the primary".

(k) Reports to Congress on sensitive queries.—Section 702(f)(3)(D) of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1881a\(f\)\(3\)\(D\)](#)) is amended by adding at the end the following:

"(vii) Reports to Congress.—Not less frequently than once each year, the Attorney General shall submit to the appropriate committees of Congress an annual report on the number of sensitive queries made in the year covered by the report, disaggregated by the subclause of clause (ii) under which the queries were approved."

(l) Repeal of expanded definition of electronic communication service provider.—

(1) Definition with respect to additional procedures regarding certain persons outside the United States.—Section 701(b)(4) of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1881\(b\)\(4\)](#)) is amended—

(A) in subparagraph (F)—

(i) by striking "custodian,"; and

(ii) by striking "(D), or (E)" and inserting "or (D)";

(B) by striking subparagraph (E);

(C) in subparagraph (D), by striking the semicolon and inserting "; or"; and

(D) by redesignating subparagraph (F) as subparagraph (E).

(2) Definition with respect to protection of persons assisting the Government.—Section 801(6) of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1885\(6\)](#)) is amended—

(A) in subparagraph (G)—

(i) by striking "custodian,"; and

(ii) by striking "(E), or (F)" and inserting "or (E)";

(B) by striking subparagraph (E);

(C) in subparagraph (F), by striking the semicolon and inserting "; or"; and

(D) by redesignating subparagraphs (F) and (G) as subparagraphs (E) and (F), respectively.

(3) Treatment of certain section 702 directives.—Any directive issued pursuant to section 702(i) of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1881a\(i\)](#)) to a person who was considered an electronic communication service provider pursuant to section 701(b)(4) of such Act ([50 U.S.C. 1881\(b\)\(4\)](#)) as such section was in effect during the period beginning on April 20, 2024, and ending on the date of enactment of this Act, but is not an electronic communication service provider pursuant to such section as in effect after the date of enactment of this Act, shall be considered null and void.

(m) Two-year extension of section 702 of the Foreign Intelligence Surveillance Act of 1978.—

(1) Extension.—Section 403(b) of the FISA Amendments Act of 2008 ([Public Law 110-261](#)) is amended—

(A) in paragraph (1) ([50 U.S.C. 1881-1881g note](#))—

(i) by striking "effective 2 years after the date of enactment of the Reforming Intelligence and Securing America Act" and inserting "effective October 30, 2028"; and

(ii) by striking "and the Reforming Intelligence and Securing America Act" and inserting ", the Reforming Intelligence and Securing America Act, and the POPULIST Act"; and

(B) in paragraph (2) ([18 U.S.C. 2511 note](#)), in the matter preceding subparagraph (A), by striking "2 years after the date of enactment of the Reforming Intelligence and Securing America Act" and inserting "October 30, 2028".

(2) Conforming amendments.—Section 404(b) of the FISA Amendments Act of 2008 ([Public Law 110-261](#); [50 U.S.C. 1801 note](#)) is amended—

(A) in paragraph (1)—

(i) in the paragraph heading, by striking "2 years after the date of enactment of the Reforming Intelligence and Securing America Act" and inserting "October 30, 2028"; and

(ii) by striking "and the Reforming Intelligence and Securing America Act" and inserting ", the Reforming Intelligence and Securing America Act, and the POPULIST Act"; and

(B) in paragraph (2), in the matter before subparagraph (A), by striking "and the Reforming Intelligence and Securing America Act" and inserting ", the Reforming Intelligence and Securing America Act, and the POPULIST Act".

SEC. 1023. FISA COURT REFORM, REMEDIES, AND EXCLUSIVE MEANS.

(a) Court supervision of collection targeting covered persons and persons located inside the United States.—

(1) In general.—Title VII of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1881 et seq.](#)) is amended—

(A) by striking sections 703, 704, and 705 ([50 U.S.C. 1881b](#), 1881c, and 1881d); and

(B) by inserting after section 702 ([50 U.S.C. 1881a](#)) the following:

"Sec. 703. Acquisitions targeting covered persons and persons located inside the United States.

"(a) Warrant requirement.—No officer or employee of the Federal Government may intentionally target a covered person for the purpose of acquiring foreign intelligence information, where such acquisition would be of communications content, location information, web browsing history, or internet search history of the covered person, or the acquisition would occur under circumstances in which the person has a reasonable expectation of privacy, or a warrant would be required for the acquisition of such information if the officer or employee sought to compel production of the information inside the United States for law enforcement purposes, unless such person is the subject of—

"(1) an order or emergency authorization under section 105 or 304 of this Act covering the period of the acquisition and the acquisition is subject to the use, dissemination, querying, retention, and other minimization limitations required by such order or authorization; or

"(2) a warrant issued pursuant to the Federal Rules of Criminal Procedure by a court of competent jurisdiction covering the period of the acquisition and the acquisition is subject to the use, dissemination, querying, retention, and other minimization limitations required by such warrant.

"(b) Use of a pen register or trap and trace device.—No officer or employee of the Federal Government may use a pen register or trap and trace device for the purpose of obtaining foreign intelligence information concerning a covered person unless—

"(1) an order or emergency authorization under section 402, 403, 105, or 304 of this Act covers the period of the acquisition and the acquisition is subject to the use, dissemination, querying, retention, and other minimization limitations required by such order or authorization; or

"(2) an order has been issued pursuant to [section 3123 of title 18](#), United States Code, by a court of competent jurisdiction covering the period of the acquisition.

"(c) Matters relating to emergency acquisition.—If an acquisition is conducted pursuant to an emergency authorization described in subsection (a)(1) or (b)(1) and the subsequent application to authorize electronic surveillance, a physical search, an acquisition, or the use of a pen register or trap and trace device is denied, or in any other case in which information is acquired in violation of subsection (a) or (b)—

"(1) no information acquired, and no evidence derived therefrom, may be used, received in evidence, or otherwise disseminated in any investigation, trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof; and

"(2) no information acquired may subsequently be used or disclosed in any other manner without the consent of such person, except with the approval of the Attorney General, if the information indicates a threat of death or serious bodily harm to any person.

"(d) Rule of construction.—Subsections (a), (b), and (c) shall apply regardless of the location of the acquisition."

(2) Conforming amendments.—The Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1801 et seq.](#)) is further amended—

(A) in section 601(a)(1) ([50 U.S.C. 1871\(a\)\(1\)](#))—

(i) by striking subparagraphs (D) through (F); and

(ii) in subparagraph (B), by striking the semicolon and inserting "; and";

(B) in section 603(b)(1) ([50 U.S.C. 1873\(b\)\(1\)](#)), in the matter before subparagraph (A), by striking "and sections 703 and 704"; and

(C) in section 706 ([50 U.S.C. 1881e](#)), by striking subsection (b).

(3) Clerical amendment.—The table of contents for the Foreign Intelligence Surveillance Act of 1978 is amended—

(A) by striking the items relating to sections 703, 704, and 705; and

(B) by inserting after the item relating to section 702 the following:

"703. Acquisitions targeting covered persons and persons located inside the United States."

(b) Consistent disclosures of relevant information in title V and other FISA applications.—

(1) Consistent procedures for title V and other FISA applications.—The Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1801 et seq.](#)) is amended in section 104(a)(12), in the matter before subparagraph (A), section 303(a)(10), in the matter before subparagraph (A), and section 402(c)(4), in the matter before subparagraph (A), by inserting ", and that the application fairly reflects all information," after "apprised of all information" each place it appears.

(2) Technical corrections.—The Foreign Intelligence Surveillance Act of 1978 is further amended—

(A) in section 104(a)—

(i) in paragraph (9), by striking "; and" and inserting a semicolon;

(ii) in paragraph (11), by striking "; and" and inserting a semicolon; and

(iii) in paragraph (12)(B), by striking the period at the end and inserting "; and";

(B) in section 303(a)—

(i) in paragraph (9), by striking "; and" and inserting a semicolon; and

(ii) in paragraph (10)(B), by striking the period at the end and inserting "; and"; and

(C) in section 502(b)(2), by redesignating subparagraphs (E) and (F) as subparagraphs (C) and (D), respectively.

(c) Strengthening accuracy procedures.—

(1) In general.—The Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1801 et seq.](#)) is amended by adding at the end the following:

"TITLE IX—REQUIRED DISCLOSURE OF RELEVANT INFORMATION

"Sec. 901. Certification regarding accuracy procedures.

"(a) Definition of accuracy procedures.—In this section, the term 'accuracy procedures' means specific procedures, adopted by the Attorney General, to ensure that an application for a court order under this Act, including any application for renewal of an existing order, is accurate and complete, including procedures that ensure, at a minimum, that—

"(1) the application reflects all information that might reasonably call into question the accuracy of the information or the reasonableness of any assessment in the application, or otherwise raises doubts about the requested findings;

"(2) the application reflects all material information that might reasonably call into question the reliability and reporting of any information from a confidential human source that is used in the application;

"(3) a complete file documenting each factual assertion in an application is maintained;

"(4) the applicant coordinates with the appropriate elements of the intelligence community (as defined in section 3 of the National Security Act of 1947 ([50 U.S.C. 3003](#))), concerning any prior or existing relationship with the target of any surveillance, search, or other means of investigation, and discloses any such relationship in the application;

"(5) before any application targeting a United States person is made, the applicant Federal officer or employee documents that the officer or employee has collected and reviewed for accuracy and completeness supporting documentation for each factual assertion in the application; and

"(6) the applicant Federal agency establishes compliance procedures for ensuring that applications are accurate and complete.

"(b) Certification.—Each application for a court order under this Act shall include a certification by the applicant that the application complies with the accuracy procedures under subsection (a).

"(c) Notice of material omission or misstatement.—If the Government learns that an application previously submitted under this Act included a material omission or misstatement, the Government shall promptly notify the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review, as applicable, and provide any correction."

(2) Clerical amendment.—The table of contents of the Foreign Intelligence Surveillance Act of 1978 is amended by adding at the end the following:

"TITLE IX—Required disclosure of relevant information

"901. Certification regarding accuracy procedures."

(3) Timeline to adopt new accuracy procedures.—

(A) In general.—Not later than 180 days after the date of enactment of this Act, the Attorney General shall issue accuracy procedures, as defined in section 901(a) of the Foreign Intelligence Surveillance Act of 1978, as added by paragraph (1).

(B) Repeal of accuracy procedures requirement from RISAA.—On the date that is 180 days after the date of enactment of this Act, paragraph (7) of section 10(a) of the Reforming Intelligence and Securing America Act ([Public Law 118–49](#); [50 U.S.C. 1804 note](#)) is repealed.

(d) Clarification regarding treatment of information and evidence acquired under the Foreign Intelligence Surveillance Act of 1978.—

(1) In general.—Section 101 of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1801](#)), as amended by this Act, is further amended by adding at the end the following:

"(t) For the purposes of notification provisions of this Act, information or evidence is 'derived' from an electronic surveillance, physical search, use of a pen register or trap and trace device, production of tangible things, or acquisition under this Act when the Government would not have originally possessed the information or evidence but for that electronic surveillance, physical search, use of a pen register or trap and trace device, production of tangible things, or acquisition, and regardless of any claim that the information or evidence is attenuated from the surveillance or search, would inevitably have been discovered, or was subsequently reobtained through other means."

(2) Policies and guidance.—

(A) In general.—Not later than 90 days after the date of enactment of this Act, the Attorney General and the Director of National Intelligence shall publish the following:

(i) Policies concerning the application of subsection (t) of section 101 of the Foreign Intelligence Surveillance Act of 1978, as added by paragraph (1).

(ii) Guidance for all members of the intelligence community, as defined in section 3 of the National Security Act of 1947 ([50 U.S.C. 3003](#)), and all Federal agencies with law enforcement responsibilities concerning the application of such subsection (t).

(B) Modifications.—Whenever the Attorney General and the Director of National Intelligence modify a policy or guidance published under subparagraph (A), the Attorney General and the Director shall publish such modifications.

(e) Sunset on grandfather clause of section 215 of the USA PATRIOT Act.—Section 102(b)(2) of the USA PATRIOT Improvement and Reauthorization Act of 2005 ([Public Law 109–177](#); [50 U.S.C. 1805 note](#)) is amended by inserting ", except that title V of the Foreign Intelligence Surveillance Act of 1978, as in effect on March 14, 2020, shall cease to have effect on the date that is 180 days after the date of enactment of this Act" after "continue in effect".

(f) Written record of Department of Justice interactions with Foreign Intelligence Surveillance Court.—Section 103 of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1803](#)) is amended by adding at the end the following:

"(n) Written record of interactions.—

"(1) Written communications.—The Attorney General shall maintain all written communications with the Foreign Intelligence Surveillance Court, including the identity of the employees of the court to or from whom the communications were made, regarding an application or order made under this title in a file associated with the application or order.

"(2) Oral communications.—The Attorney General shall—

"(A) document a summary of any oral communications with the Foreign Intelligence Surveillance Court, including the identity of the employees of the court to or from whom the communications were made, relating to an application or order described in paragraph (1); and

"(B) keep such documentation in a file associated with the application or order."

(g) Appointment of amici curiae and access to information.—

(1) Expansion of appointment authority.—Section 103(i) of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1803\(i\)](#)) is amended—

(A) in paragraph (2)—

(i) in subparagraph (A)—

(I) by striking clause (i) and inserting the following:

"(i) shall appoint 1 or more individuals who have been designated under paragraph (1) and who possess expertise in privacy and civil liberties to serve as amicus curiae to assist such court in the consideration of any application or motion for an order or review, unless the court issues a written finding that such application neither presents nor involves—

"(I) a novel or significant interpretation of the law;

"(II) a significant concern related to constitutional rights;

"(III) a sensitive investigative matter;

"(IV) a request for approval of a new program, a new technology, or a new use of existing technology;

"(V) a request for reauthorization of programmatic surveillance; or

"(VI) any other privacy or civil liberties issue for which an appointment of an amicus curiae to assist the court in the consideration of the application would be appropriate;";

(II) in clause (ii), by striking "; and" and inserting a period;

(III) by redesignating clause (ii) as clause (iv) and moving such clause so as to appear after clause (iii); and

(IV) by inserting after clause (i) the following:

"(ii) shall appoint 1 or more individuals who have been designated under paragraph (1) and who possess technical expertise to serve as amicus curiae to assist such court in the consideration of any application for an order or review, unless the court issues a written finding that such application neither presents nor involves—

"(I) a request for approval of a new program, a new technology, or a new use of existing technology;

"(II) a request for approval of a previously authorized program, technology, or use of existing technology for which no prior application for approval of such program, technology, or use was considered by the court with the assistance of an amicus curiae who possesses technical expertise; or

"(III) a technical issue material to any legal determination for which an appointment of an amicus curiae who possesses technical expertise to assist the court in the consideration of the application would be appropriate;" and

(V) in clause (iii), by striking ", unless the court issues a finding that such appointment is not appropriate or is likely to result in undue delay." and inserting "; and"; and

(ii) by striking subparagraph (B);

(B) by adding at the end the following:

"(12) Definition of sensitive investigative matter.—In this subsection, the term 'sensitive investigative matter' means—

"(A) an investigative matter involving the activities of—

"(i) a domestic public official or political candidate, or an individual serving on the staff of such an official or candidate;

"(ii) a domestic religious or political organization, or a known or suspected United States person prominent in such an organization; or

"(iii) the domestic news media; or

"(B) any other investigative matter involving a domestic entity or a known or suspected United States person that, in the judgment of the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review, is similarly as sensitive as an investigative matter described in subparagraph (A)."; and

(C) in paragraph (3)(A)—

(i) by inserting "cybersecurity, cryptography," after "communications technology," and

(ii) by adding at the end the following: "Of such individuals, at least 1 shall possess legal expertise and at least 1 shall possess technical expertise.".

(2) Authority to seek review.—Section 103(i) of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1803\(i\)](#)), as amended by paragraph (1), is further amended—

(A) in paragraph (4)—

(i) in the paragraph heading, by inserting "; authority" after "Duties";

(ii) in the matter preceding subparagraph (A), by striking "shall";

(iii) in subparagraph (B)—

(I) in the matter preceding clause (i), by inserting "shall" before "provide";

(II) in clause (i), by striking "of United States persons" and inserting ", including legal arguments regarding any privacy or civil liberties interest of any United States person that would be significantly affected by the application or motion"; and

(III) in clause (iii), by striking the period at the end and inserting "; and";

(iv) by striking subparagraph (A);

(v) by redesignating subparagraph (B) as subparagraph (A); and

(vi) by adding at the end the following:

"(B) may seek leave to raise any novel or significant privacy or civil liberties issue relevant to the application or motion or other issue directly affecting the legality of the proposed electronic surveillance with the court, regardless of whether the court has requested assistance on that issue.";

(B) by redesignating paragraphs (7) through (12) as paragraphs (8) through (13), respectively; and

(C) by inserting after paragraph (6) the following:

"(7) Authority to seek review of decisions.—

"(A) Foreign Intelligence Surveillance Court decisions.—

"(i) Petition.—Following issuance of an order under this Act by the Foreign Intelligence Surveillance Court, an amicus curiae appointed under paragraph (2) may petition the Foreign Intelligence Surveillance Court to certify for review to the Foreign Intelligence Surveillance Court of Review a question of law pursuant to subsection (j).

"(ii) Denials.—If the Foreign Intelligence Surveillance Court denies a petition described in clause (i), the court shall provide for the record a written statement of the reasons for such denial.

"(iii) Certification.—Upon certification of any question of law pursuant to this subparagraph, the Foreign Intelligence Surveillance Court of Review shall appoint the amicus curiae to assist the Court of Review in its consideration of the certified question, unless the Court of Review issues a finding that such appointment is not appropriate.

"(B) Foreign Intelligence Surveillance Court of Review decisions.—An amicus curiae appointed under paragraph (2) may petition the Foreign Intelligence Surveillance Court of Review to certify for review to the Supreme Court of the United States any question of law pursuant to [section 1254\(2\) of title 28](#), United States Code.

"(C) Declassification of referrals.—For purposes of section 602, a petition filed under subparagraph (A) or (B) of this paragraph and all of its content shall be considered a decision, order, or opinion issued by the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review described in paragraph (2) of section 602(a)."

(3) Access to information.—Section 103(i)(6) of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1803\(i\)\(6\)](#)) is amended—

(A) in subparagraph (A), by striking clauses (i) and (ii) and inserting the following:

"(i) shall have access to, to the extent such information is available to the Government—

"(I) the application, certification, petition, motion, and other information and supporting materials, including any information described in section 901, submitted to the Foreign Intelligence Surveillance Court in connection with the matter in which the amicus curiae has been appointed, including access to any relevant legal precedent, including any such precedent that is cited by the Government, including in such an application;

"(II) any other information or materials that the court determines is relevant to the duties of the amicus curiae; and

"(III) an unredacted copy of each relevant decision made by the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review in which the court decides a question of law, without regard to whether the decision is classified; and

"(ii) may make a submission to the court requesting access to any other particular materials or information, or category of materials or information, that the amicus curiae believes to be relevant to the duties of the amicus curiae.";

(B) by redesignating subparagraph (D) as subparagraph (F); and

(C) by inserting after subparagraph (C) the following:

"(D) Supporting documentation regarding accuracy.—The Foreign Intelligence Surveillance Court, upon the motion of an amicus curiae appointed under paragraph (2) or upon its own motion, may require the Government to make available the supporting documentation described in section 901.".

(4) Clarification of access to certain information.—Section 103(i)(6) of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1803\(i\)\(6\)](#)) is amended—

(A) in subparagraph (B), by striking "The Attorney General may periodically" and inserting "Not less frequently than annually, the Attorney General shall"; and

(B) by striking subparagraph (C) and inserting the following:

"(C) Classified information.—An amicus curiae appointed by the court shall have access to, to the extent such information is available to the Government, unredacted copies of each opinion, order, transcript, pleading, or other document of the Foreign Intelligence Surveillance Court and the Foreign Intelligence Surveillance Court of Review, including, if the individual is eligible for access to classified information, any classified documents, information, and other materials or proceedings.".

(5) Consultation among amici curiae.—Section 103(i)(6) of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1803\(i\)\(6\)](#)), as amended by paragraphs (3) and (4), is further amended—

(A) by redesignating subparagraphs (B), (C), and (D) as subparagraphs (C), (D), and (E), respectively; and

(B) by inserting after subparagraph (A) the following:

"(B) Consultation.—If the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review determines that it is relevant to the duties of an amicus curiae appointed under paragraph (2), the amicus curiae may consult with 1 or more of the other individuals designated to serve as amicus curiae under paragraph (1) regarding any of the information relevant to any assigned proceeding."

(6) Notification.—Section 103(i), as amended by paragraphs (1) and (2), is further amended by striking paragraph (8), as redesignated by paragraph (2)(B), and inserting the following:

"(8) Notification.—A presiding judge of the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review shall, not less frequently than quarterly, provide to the Attorney General and the appropriate committees of Congress—

"(A) a notification of each appointment of an individual to serve as amicus curiae under paragraph (2); and

"(B) a copy of each written finding issued under paragraph (2)."

(7) Section 702 recertification schedule.—Section 702(j)(5)(A) of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1881a\(j\)\(5\)\(A\)](#)) is amended by striking "at least 30 days prior to the expiration of such authorization" and inserting "such number of days, not less than 30 days, before the expiration of such authorization as the Court considers necessary to permit review by amici curiae appointed under section 103(i)(2)(A)(iii)."

(h) Declassification of significant decisions, orders, and opinions.—Section 602(a) of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1872\(a\)](#)) is amended to read as follows:

"(a) Declassification required.—

"(1) In general.—Subject to subsection (b), the Director of National Intelligence, in consultation with the Attorney General, shall—

"(A) conduct a declassification review of each decision, order, or opinion issued by the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review, as defined in section 601(e), that is described in paragraph (2);

"(B) consistent with that review, make publicly available to the greatest extent practicable each such decision, order, or opinion; and

"(C) for any such decision, order, or opinion issued after the date of enactment of this section, complete the declassification review and public release by not later than 180 days

after the date on which the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review issues such decision, order, or opinion.

"(2) Decision, order, or opinion described.—A decision, order, or opinion issued by the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review that is described in this paragraph is any such decision, order, or opinion issued before, on, or after the date of enactment of this Act, that—

"(A) includes a significant construction or interpretation of any provision of law, including any novel or significant construction or interpretation of any term;

"(B) involves a sensitive investigative matter, as defined in section 103(i)(13); or

"(C) has been nominated for a declassification review by an amicus curiae appointed by the court."

(i) Clarification of Foreign Intelligence Surveillance Court jurisdiction over records of the court and other ancillary matters.—

(1) In general.—Section 103 of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1803](#)) is amended—

(A) by adding at the end the following:

"(o) Ancillary claims.—

"(1) Foreign Intelligence Surveillance Court.—The Foreign Intelligence Surveillance Court shall have jurisdiction to hear claims ancillary to any of its own proceedings, including jurisdiction to hear any claim for access to the court's records, files, and proceedings under the Constitution of the United States, statute, common law, or any other authority. Upon deciding such a claim, the Court shall provide immediately for the record a written statement of the reasons for such decision. A party may file a petition for review of such decision with the Foreign Intelligence Surveillance Court of Review, which shall have jurisdiction to consider such petition and, upon deciding such petition, shall provide for the record a written statement of the reasons for its decision.

"(2) Foreign Intelligence Surveillance Court of Review.—The Foreign Intelligence Surveillance Court of Review shall have jurisdiction to hear claims ancillary to any of its own proceedings, including jurisdiction to hear any claim for access to the court's records, files, and proceedings under the Constitution of the United States, statute, common law, or any other authority. Upon deciding such a claim, the Court of Review shall provide immediately for the record a written statement of the reasons for such decision.

"(3) Supreme Court review.—A party may file a petition for a writ of certiorari for review of a decision of the Foreign Intelligence Surveillance Court of Review under paragraphs (1) or (2), and the Supreme Court shall have jurisdiction to review such decision.";

(B) in subsection (a)(2)(A), in the matter preceding clause (i), by inserting "paragraph (1) of subsection (o) of this section or" before "paragraph (4) or (5) of section 702(i)"; and

(C) in subsection (k)(1), by striking "[section 1254\(2\) of title 28](#)" and inserting "[section 1254 of title 28](#)".

(2) Technical corrections.—Section 103 of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1803](#)), as amended by paragraph (1), is further amended—

(A) in subsection (a)(2)(A), in the matter preceding clause (i), by striking "section 501(f) or"; and

(B) in subsection (e), by striking "section 501(f)(1) or" each place it appears.

(j) Grounds for determining injury in fact in civil actions relating to surveillance under the Foreign Intelligence Surveillance Act of 1978 or pursuant to executive authority.—

(1) In general.—The Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1801 et seq.](#)), as amended by this section, is further amended by adding at the end the following new title:

"TITLE X—ADDITIONAL MATTERS

"SEC. 1001. Challenges to Government surveillance.

"SEC. 1002. Accountability procedures for violations by Federal employees.

"Sec. 1001. Challenges to Government surveillance.

"(a) Definitions.—In this section, the terms 'foreign intelligence information', 'person', 'United States', and 'United States person' have the meanings given such terms in section 101.

"(b) Injury in fact.—In any claim in a civil action brought in a court of the United States relating to the acquisition, copying, querying, retention, access, or use of information acquired under this Act or pursuant to any other authority of the executive branch of the Federal Government, by a United States person or person located inside the United States, the person asserting the claim has suffered an injury in fact traceable to that conduct if the person—

"(1) (A) regularly communicates foreign intelligence information with persons who are not United States persons and who are located outside the United States; and

"(B) has taken or is taking objectively reasonable measures to avoid the acquisition, copying, querying, retention, access, or use of the person's information under this Act or pursuant to another authority of the executive branch of the Federal Government; or

"(2) has a reasonable basis to believe that the person's rights have been, are being, or imminently will be violated by an individual acting under color of Federal law.

"(c) Reasonable basis.—For the purposes of this section, a reasonable basis exists when the person demonstrates a concrete injury arising from a good-faith belief that the person's rights have been, are being, or imminently will be violated through the acquisition, copying, querying, retention, access, or use of the person's information under this Act or pursuant to any other authority of the executive branch of the Federal Government.

"(d) State secrets privilege.—The procedures set forth in section 106(f) shall apply when the state secrets privilege is asserted, with respect to any claim where the plaintiff, who is a United States person or person located in the United States, plausibly alleges an injury in fact relating to the acquisition, copying, querying, retention, access, or use of information acquired under this Act or pursuant to another authority of the executive branch of the Federal Government and plausibly alleges that the acquisition, copying, querying, retention, access, or use of information violates the Constitution or laws of the United States.

"Sec. 1002. Accountability procedures for violations by Federal employees.

"(a) Definitions.—In this section:

"(1) Appropriate committees of Congress.—The term 'appropriate committees of Congress' has the meaning given such term in section 101.

"(2) Covered agency.—The term 'covered agency' means the Federal Bureau of Investigation, the Central Intelligence Agency, the National Security Agency, and the National Counterterrorism Center.

"(3) Covered person.—The term 'covered person' has the meaning given such term in section 701(b).

"(4) Covered violation.—The term 'covered violation' means a violation of this Act, the POPULIST Act, or Executive Order 12333 ([50 U.S.C. 3001 note](#); relating to United States intelligence activities), or successor order, by an employee of a covered agency that results in the inappropriate collection, use, querying, or dissemination of any communication, record, or information of a covered person.

"(5) Person, United States, and United States person.—The terms 'person', 'United States', and 'United States person' have the meanings given such terms in section 101.

"(b) Accountability procedures; designated investigative entity.—The head of each covered agency shall—

"(1) establish procedures to hold employees of the covered agency accountable for willful, knowing, reckless, and negligent covered violations; and

"(2) (A) designate an entity within the agency to investigate possible willful, knowing, reckless, and negligent covered violations; and

"(B) establish an internal process for the designated entity to determine culpability for willful, knowing, reckless, and negligent covered violations.

"(c) Elements.—The procedures established under subsection (b)(1) shall include the following:

"(1) Centralized tracking of individual employee performance incidents involving willful, knowing, reckless, and negligent covered violations, over time.

"(2) Escalating consequences for willful, knowing, reckless, and negligent covered violations, including—

"(A) consequences for an initial reckless or negligent covered violation, including, at a minimum—

"(i) suspension of access to information acquired under this Act or to the dataset that gave rise to the violation for not less than 90 days; and

"(ii) documentation of the incident in the personnel file of each employee responsible for the violation;

"(B) consequences for a 2nd reckless or negligent covered violation, including, at a minimum—

"(i) suspension of access to information acquired under this Act or to the dataset that gave rise to the violation for not less than 180 days; and

"(ii) reassignment of each employee responsible for the violation;

"(C) consequences for a 3rd reckless or negligent covered violation, including, at a minimum—

"(i) termination of security clearance; and

"(ii) reassignment or termination of each employee responsible for the violation;

"(D) consequences for an initial willful or knowing covered violation, including, at a minimum—

"(i) suspension of access to information acquired under this Act or to the dataset that gave rise to the violation for not less than 180 days; and

"(ii) reassignment of each employee responsible for the violation; and

"(E) consequences for a 2nd willful or knowing covered violation, including, at a minimum—

"(i) termination of security clearance; and

"(ii) reassignment or termination of each employee responsible for the violation.

"(d) Presumption of termination.—

"(1) In general.—For purposes of subparagraphs (C)(ii) and (E)(ii) of subsection (c)(2), there shall be a presumption in favor of termination of an employee.

"(2) Justification.—If the head of a covered agency determines not to terminate an employee for a 3rd reckless or negligent violation under subparagraph (C)(ii) of subsection (c)(2) or a 2nd willful or knowing violation under subparagraph (E)(ii) of that subsection, the agency head shall submit to the appropriate committees of Congress a written justification for the determination.

"(e) Timing.—If a covered agency determines, through an investigation, that an employee committed a willful, knowing, reckless, or negligent covered violation, the agency head shall

determine what consequences to impose on the employee under subsection (c)(2) not later than 60 days after the conclusion of the investigation."

(2) Report required.—

(A) In general.—Not later than 180 days after the date of enactment of this Act, the head of each covered agency, as defined in section 1002 of the Foreign Intelligence Surveillance Act of 1978, as added by paragraph (1), shall submit to the appropriate committees of Congress a report detailing—

(i) the procedures established under section 1002 of the Foreign Intelligence Surveillance Act of 1978, as added by paragraph (1); and

(ii) a description of any actions taken pursuant to such procedures.

(B) Form.—The report required by subparagraph (A) shall be submitted in unclassified form, but may include a classified annex to the extent necessary to protect sources and methods.

(3) Deconfliction with RISAA accountability procedures.—

(A) In general.—Paragraph (4) of section 702(f) of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1881a\(f\)](#)) is repealed.

(B) Conforming amendment.—Paragraph (6) of such section 702(f), as added by section 1022(a) of this Act, is redesignated as paragraph (4) and moved before paragraph (5) of such section 702(f).

(C) Effective date.—The amendments made by subparagraphs (A) and (B) shall take effect on the date that is 180 days after the date of enactment of this Act.

(k) Reforms to the exclusive means limitations under the Foreign Intelligence Surveillance Act of 1978.—

(1) [Chapter 119 of title 18](#).—[Section 2511\(2\)\(f\) of title 18](#), United States Code, as amended by this Act, is further amended to read as follows:

"(f) (i) Other than as provided in subparagraph (ii), nothing contained in this chapter or chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934 ([47 U.S.C. 605](#)), shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1801](#)).

"(ii) The procedures in this chapter, chapter 121, and the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1801 et seq.](#)) shall be the exclusive means by which the United States Government may conduct—

"(A) electronic surveillance, as defined in section 101 of that Act;

"(B) the interception of wire, oral, and electronic communications within the United States or from a domestic electronic communications system; or

"(C) the interception of wire, oral, and electronic communications for which the sender and all intended recipients are located within the United States.".

(2) Foreign Intelligence Surveillance Act.—Section 112 of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1812](#)) is amended to read as follows:

"(a) Except as provided in subsection (b), the procedures of chapters 119, 121, and 206 of title 18 and this Act shall be the exclusive means by which the United States Government may conduct—

"(1) electronic surveillance, as defined in section 101;

"(2) the interception of wire, oral, and electronic communications within the United States or from a domestic electronic communications system; or

"(3) the interception of wire, oral, and electronic communications for which the sender and all intended recipients are located within the United States.

"(b) Only an express statutory authorization for electronic surveillance or the interception of wire, oral, or electronic communications described in subsection (a), other than as an amendment to this chapter or chapters 119, 121, or 206 of title 18, shall constitute an additional exclusive means for the purpose of subsection (a).

"(c) The procedures in this Act and section 1024 of the POPULIST Act shall be the exclusive means by which the location information of 1 or more persons located in the United States may be acquired for foreign intelligence purposes by the United States Government.".

SEC. 1024. NON-FISA FOREIGN INTELLIGENCE SURVEILLANCE REFORM.

(a) Definitions.—In this section:

(1) Congressional intelligence committees, foreign intelligence, intelligence, and intelligence community.—The terms "congressional intelligence committees", "foreign intelligence", "intelligence", and "intelligence community" have the meanings given such terms in section 3 of the National Security Act of 1947 ([50 U.S.C. 3003](#)).

(2) Covered person.—The term "covered person" has the meaning given such term in section 701(b) of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1881\(b\)](#)), as amended by this Act.

(3) Electronic surveillance, person, State, United States, and United States person.—The terms "electronic surveillance", "person", "State", "United States", and "United States person" have the meanings given such terms in section 101 of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1801](#)).

(b) Protections related to warrantless queries.—

(1) Definitions.—In this subsection:

(A) Covered information.—The term "covered information" includes—

- (i) communications content; and
- (ii) information, the compelled disclosure of which would require a probable cause warrant if sought for law enforcement purposes inside the United States.

(B) Covered query.—The term "covered query" means a query—

- (i) using a term associated with 1 or more covered persons; or
- (ii) for a significant purpose of retrieving information of, or concerning, 1 or more covered persons.

(C) Query.—The term "query" means the use of 1 or more terms, whether conducted through manual or automated means, to retrieve information acquired for foreign intelligence purposes, other than acquisitions authorized by the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1801 et seq.](#)), including retrieval from a subset of such information, whether that subset was created by retrieval through a query or other means, regardless of whether such acquisition occurred inside or outside the United States.

(2) In general.—Except as provided in paragraphs (3) and (4), no officer or employee of the Federal Government may access covered information returned in response to a covered query.

(3) Exceptions for concurrent authorization, consent, emergency situations, and certain defensive cybersecurity queries.—Paragraph (2) shall not apply if—

(A) the covered person to whom the covered query relates is the subject of an order or emergency authorization authorizing electronic surveillance or physical search under section 105 or 304 of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1805, 1824](#)), or a warrant issued pursuant to the Federal Rules of Criminal Procedure by a court of competent jurisdiction, if—

- (i) such order, authorization, or warrant covers the period of the covered query; and
- (ii) the covered query is conducted and covered information is accessed in compliance with all use, dissemination, querying, retention, and other minimization limitations required by the order, authorization, or warrant;

(B) (i) the officer or employee accessing the covered information has a reasonable belief that—

(I) an emergency exists involving an imminent threat of death or serious bodily harm; and

(II) in order to prevent or mitigate the threat described in subclause (I), the query must be conducted before authorization described in subparagraph (A) can, with due diligence, be obtained; and

(ii) not later than 14 days after the covered information is accessed, a description of the circumstances justifying the accessing of the covered information is provided to the congressional intelligence committees in a timely manner;

(C) the covered person to whom the covered query relates or, if such person is incapable of providing consent, a third party legally authorized to consent on behalf of the person, has provided consent for such access on a case-by-case basis; or

(D) (i) the covered information is used for defensive cybersecurity purposes, including the protection of a covered person from cybersecurity attack;

(ii) other than for such defensive cybersecurity purposes, no covered information is accessed or reviewed; and

(iii) not later than 14 days after the covered information is accessed, a description of the circumstances justifying the accessing of the covered information is provided to the congressional intelligence committees.

(4) Matters relating to emergency queries.—

(A) Treatment of denials.—If covered information is accessed pursuant to an emergency authorization described in paragraph (3)(A) and the subsequent application to authorize electronic surveillance, a physical search, or an acquisition pursuant to section 105(e) or 304(e) of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1805\(e\)](#), 1824(e)) is denied, or in any other case in which covered information is accessed in violation of this subsection—

(i) no covered information accessed, or evidence derived from such access, may be used, received in evidence, or otherwise disseminated in any investigation, trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof; and

(ii) no covered information accessed, or evidence derived from such access, concerning a covered person may subsequently be used or disclosed in any other manner without the consent of such covered person, except if the Attorney General approves the use or disclosure of such covered information in order to prevent the death of or serious bodily harm to any person.

(B) Assessment of compliance.—Not less frequently than annually, the Attorney General shall assess compliance with the requirements under subparagraph (A).

(5) Foreign Intelligence Surveillance Act of 1978.—This subsection shall not apply to the access of covered information collected pursuant to the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1801 et seq.](#)).

(6) Foreign intelligence purpose required for queries.—

(A) In general.—Except as provided in subparagraph (B), no officer or employee of the Federal Government may conduct a query unless the query is—

(i) reasonably likely to retrieve foreign intelligence information; and

(ii) made with a significant foreign intelligence purpose.

(B) Exceptions.—An officer or employee of the Federal Government is permitted to conduct a query if an exception described in clauses (i) and (ii) of section 702(f)(2)(B) of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1881a\(f\)\(2\)\(B\)](#)), as amended by section 1022 of this Act, applies.

(7) Documentation.—No officer or employee of the Federal Government may conduct a covered query, or access covered information returned in response to a covered query, unless an electronic record is created that includes—

(A) for each query—

- (i) each term used for the conduct of the query;
- (ii) the date of the covered query;
- (iii) the identifier of the officer or employee who conducted the covered query; and
- (iv) (I) a statement of facts justifying that the query is reasonably likely to retrieve foreign intelligence information and the significant foreign intelligence purpose for the query; or
(II) an exception under paragraph (6)(B) applies and a description of the basis for the exception; and

(B) for each access—

- (i) the date of the access;
- (ii) the identifier of the officer or employee who did the particular access; and
- (iii) a statement of facts showing that an access is authorized by an exception under paragraph (3).

(8) Query record system.—

(A) In general.—The head of each agency that may conduct a covered query shall ensure that a system, mechanism, or business practice is in place to maintain the records described in paragraph (7), including ensuring that any covered queries, or accesses to covered information returned in response to covered queries, that are conducted by automated means are attributed to the officer or employee who was the proximate cause of such covered query or access.

(B) Compliance report.—Not later than 90 days after the date of enactment of this Act, the head of each agency that may conduct a covered query shall report to the congressional intelligence committees on its compliance with subparagraph (A).

(c) Prohibition on reverse targeting of covered persons.—

(1) Prohibition on acquisition.—No officer or employee of the Federal Government may intentionally target, for the purpose of acquiring foreign intelligence information, any person to acquire information, regardless of whether such targeting or acquisition occurs inside or outside

the United States, if a significant purpose of the acquisition is to acquire the information of a particular, known covered person, unless—

(A) (i) the officer or employee has a reasonable belief that an emergency exists involving a threat of imminent death or serious bodily harm to such covered person;

(ii) the information is sought for the purpose of assisting that person; and

(iii) not later than 14 days after the targeting, a description of the targeting is provided to the congressional intelligence committees in a timely manner; or

(B) the covered person has provided consent to the targeting, or if such covered person is incapable of providing consent, a third party legally authorized to consent on behalf of such covered person has provided consent.

(2) Foreign Intelligence Surveillance Act of 1978 and criminal warrants.—This subsection shall not apply to—

(A) an acquisition carried out pursuant to the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1801 et seq.](#)); or

(B) an acquisition carried out pursuant to a warrant issued pursuant to the Federal Rules of Criminal Procedure by a court of competent jurisdiction covering the period of the acquisition and the acquisition is subject to the use, dissemination, querying, retention, and other minimization limitations required by such warrant.

(d) Prohibition on intelligence acquisition of covered person data.—

(1) Covered data defined.—In this subsection, the term "covered data"—

(A) means data, derived data, or any unique identifier that is linked to or is reasonably linkable to a covered person or to an electronic device that is linked to, or is reasonably linkable to, 1 or more covered persons in a household;

(B) includes anonymized data that, if combined with other data, can be linked to, or is reasonably linkable to, a covered person or to an electronic device that is linked to, or is reasonably linkable to, 1 or more covered persons in a household; and

(C) does not include data that—

(i) is lawfully available to the public through Federal, State, or local government records or through widely distributed media;

(ii) is reasonably believed to have been voluntarily made available to the general public by the covered person; or

(iii) is a specific communication or transaction with a targeted individual who is not a covered person.

(2) Limitation.—

(A) In general.—Subject to subparagraphs (B) through (H), an element of the intelligence community may not acquire a dataset that includes covered data.

(B) Authorization pursuant to the Foreign Intelligence Surveillance Act of 1978.—An element of the intelligence community may acquire covered data if the data has been authorized for collection pursuant to an order or emergency authorization pursuant to the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1801 et seq.](#)) or the Federal Rules of Criminal Procedure by a court of competent jurisdiction covering the period of the acquisition, subject to the use, dissemination, querying, retention, and other minimization limitations required by such authorization.

(C) Authorization for employment-related use.—An element of the intelligence community may acquire covered data about an employee of, or applicant for employment by, an element of the intelligence community for employment-related purposes, provided that—

(i) access to and use of the covered data is limited to such purposes; and

(ii) the covered data is destroyed at such time as it is no longer necessary for such purposes.

(D) Exception for compliance purposes.—An element of the intelligence community may acquire covered data for the purpose of supporting compliance with collection limitations and minimization requirements imposed by statute, guidelines, procedures, or the United States Constitution, provided that—

(i) access to and use of the covered data is limited to such purpose; and

(ii) the covered data is destroyed at such time as it is no longer necessary for such purpose.

(E) Exception for life or safety.—An element of the intelligence community may acquire covered data if—

(i) (I) there is a reasonable belief that an emergency exists involving an imminent threat of death or serious bodily harm; and

(II) in order to prevent or mitigate this threat, the acquisition must be conducted before authorization pursuant to subparagraph (B) can, with due diligence, be obtained;

(ii) access to and use of the covered data is limited to addressing the threat;

(iii) the covered data is destroyed at such time as it is no longer necessary for such purpose; and

(iv) not later than 14 days after the acquisition, a description of the acquisition is provided to the congressional intelligence committees.

(F) Exception for consent.—An element of the intelligence community may acquire covered data if—

(i) each covered person linked or reasonably linked to the covered data, or, if such person is incapable of providing consent, a third party legally authorized to consent on behalf of the person, has provided consent to the acquisition and use of the data on a case-by-case basis;

(ii) access to and use of the covered data is limited to the purposes for which the consent was provided; and

(iii) the covered data is destroyed at such time as it is no longer necessary for such purposes.

(G) Exception for nonsegregable data.—An element of the intelligence community may acquire a dataset that includes covered data if the covered data is not reasonably segregable prior to acquisition, provided that the element of the intelligence community complies with the minimization procedures in paragraph (3).

(H) Exception for national security letter data.—An element of the intelligence community may acquire, through noncompulsory means that are otherwise not contrary to a provision of Federal law, data that, in the United States, the Federal Government has the authority to compel production through a national security letter pursuant to [section 2709 of title 18](#), United States Code, section 626 or 627 of the Consumer Credit Protection Act ([15 U.S.C. 1681u](#), 1681v), or section 1114 of the Right to Financial Privacy Act of 1978 ([12 U.S.C. 3414](#)), provided—

(i) the person or entity in possession of the data is outside the United States and compelled production is not feasible;

(ii) the acquisition is conducted consistent with the limitations that would apply if, in the United States, the Federal Government compelled production of such data with a national security letter pursuant to such provisions of law; and

(iii) the element of the intelligence community maintains all records required by such provisions of law, including the content of relevant certifications, for each covered person or each instance of data, derived data, or unique identifier linked to or reasonably linkable to a covered person.

(3) Minimization procedures.—

(A) In general.—The Attorney General shall adopt specific procedures that are reasonably designed to minimize the acquisition and retention of covered data that is not subject to 1 or more of the exceptions set forth in paragraph (2).

(B) Acquisition and retention.—The procedures adopted under subparagraph (A) shall require elements of the intelligence community to exhaust all reasonable means—

(i) to exclude covered data not subject to 1 or more exceptions set forth in paragraph (2) from datasets prior to acquisition; and

(ii) to remove and delete covered data not subject to 1 or more exceptions set forth in paragraph (2) prior to the operational use of the acquired dataset or the inclusion of the dataset in a database intended for operational use.

(C) Destruction.—The procedures adopted under subparagraph (A) shall require that if an element of the intelligence community identifies covered data acquired in violation of paragraph (2), such covered data shall be promptly destroyed.

(4) Prohibition on use of data obtained in violation of this subsection.—Covered data acquired by an element of the intelligence community in violation of paragraph (2), and any evidence derived therefrom, may not be used, received in evidence, or otherwise disseminated in any investigation, trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof.

(5) Reporting requirement.—

(A) In general.—Not later than 180 days after the date of enactment of this Act, and not less frequently than once each year thereafter, the Director of National Intelligence shall submit to the appropriate committees of Congress and the Privacy and Civil Liberties Oversight Board a report on acquisitions pursuant to this subsection.

(B) Contents.—The report submitted pursuant to subparagraph (A) shall include the following:

(i) Datasets.—A description of datasets that the Director determines contain information of covered persons that is significant in volume proportion, or sensitivity, including—

(I) the covered person information in each dataset; and

(II) an estimate of the amount of covered person information in each dataset.

(ii) Data collection.—A description of data collected pursuant to paragraph (2)(H), including—

(I) a description of the covered person information for each acquisition; and

(II) the number of covered persons or instances of data, derived data, or unique identifiers linked to or reasonably linkable to a covered person, disaggregated by the national security letter authority for which compelled production would be required.

(iii) Detected violations.—A description of covered data identified as having been acquired in violation of paragraph (2) in the preceding year, including—

(I) an estimate of the number of covered persons whose information was acquired in violation of paragraph (2); and

(II) any changes made to the procedures in paragraph (3) to address compliance issues.

(C) Notifications.—After submitting the report required by subparagraph (A), the Director shall, in coordination with the Under Secretary of Defense for Intelligence and Security, notify the appropriate committees of Congress of any changes to the information contained in such report.

(D) Availability to the public.—The Director shall make available to the public on the website of the Director—

- (i) the unclassified portion of the report submitted pursuant to subparagraph (A); and
- (ii) any notifications submitted pursuant to subparagraph (C).

(6) Rule of construction.—Nothing in this subsection shall authorize an acquisition otherwise prohibited by this Act, the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1801 et seq.](#)), or title 18, United States Code.

(e) Prohibition on the warrantless acquisition of domestic communications.—No officer or employee of the Federal Government may intentionally acquire, for the purpose of acquiring foreign intelligence information, any communication as to which the sender and all intended recipients are known to be located in the United States at the time of acquisition or the time of communication, regardless of whether such acquisition occurs inside or outside the United States, except—

(1) as authorized under section 105 or 304 of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1805](#), 1824); or

(2) if—

(A) the officer or employee has a reasonable belief that—

(i) an emergency exists involving the imminent threat of death or serious bodily harm; and

(ii) in order to prevent or mitigate this threat, the acquisition must be conducted before an authorization pursuant to the provisions of law cited in paragraph (1) can, with due diligence, be obtained; and

(B) not later than 14 days after the acquisition, a description of the acquisition is provided to the congressional intelligence committees.

(f) Data retention limits.—

(1) Procedures.—

(A) In general.—Each head of an element of the intelligence community shall develop and implement procedures governing the retention of information described in subparagraph (B).

(B) Information described.—The information described in this subparagraph is information that was acquired for foreign intelligence purposes, other than acquisitions authorized by the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1801 et seq.](#)), regardless of whether such acquisition occurred inside or outside the United States.

(2) Requirements.—

(A) Covered information defined.—In this paragraph, the term "covered information" includes—

(i) any information or communication pertaining to a covered person, including an encrypted communication to or from a covered person, that has been evaluated and is not specifically known to contain foreign intelligence information; and

(ii) any unevaluated information, unless it can reasonably be determined that the unevaluated information does not contain any information or communications pertaining to a covered person, including any encrypted communication to or from a covered person.

(B) In general.—The procedures developed and implemented pursuant to paragraph (1) shall ensure, with respect to information described in such paragraph, that covered information shall be destroyed within 5 years of collection unless the Attorney General determines in writing that—

(i) the information is the subject of a preservation obligation in pending administrative, civil, or criminal litigation, in which case the covered information shall be segregated, retained, and used solely for that purpose and shall be destroyed as soon as it is no longer required to be preserved for such litigation; or

(ii) the information is being used in a proceeding or investigation consistent with section 706(a) of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1881e\(a\)](#)).

(g) Reports on violations of law or Executive order.—Section 511 of the National Security Act of 1947 ([50 U.S.C. 3110](#)) is amended by adding at the end the following:

"(c) Public availability.—

"(1) In general.—The Director of National Intelligence shall make each report submitted under subsection (a) publicly available on an internet website, with such redactions as may be necessary to protect sources and methods.

"(2) Retroactive report publication.—With respect to a report submitted under subsection (a) prior to the date of enactment of this Act, such report shall be made publicly available pursuant to paragraph (1) by not later than 180 days after the date of enactment of this Act.

"(d) Department of Justice report.—The Attorney General, in consultation with the Director of National Intelligence, shall submit to the Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives a version of the report described in subsection (a) that only addresses violations of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1801 et seq.](#)).".

SEC. 1025. SURVEILLANCE OVERSIGHT AND INTELLIGENCE TRANSPARENCY.

(a) Inspector General oversight of orders under the Foreign Intelligence Surveillance Act of 1978.—

(1) Audit.—Not later than July 1, 2027, the Inspector General of the Department of Justice and the Inspector General of each element of the intelligence community shall each initiate an audit of the applications for court orders made under the Foreign Intelligence Surveillance Act

of 1978 ([50 U.S.C. 1801 et seq.](#)) and directives issued under section 702(i) of such Act by the Department or the element, respectively.

(2) Scope and contents.—In conducting an audit under paragraph (1)—

(A) an Inspector General shall—

(i) review such sample of applications and directives described in paragraph (1) as the Inspector General determines appropriate in order to carry out the objectives of this subsection;

(ii) assess whether—

(I) adequate safeguards are in place to ensure that the assertions made in applications are scrupulously accurate;

(II) adequate safeguards are in place to ensure that each application includes all information required by the amendments made by section 10 of the Reforming Intelligence and Securing America Act ([Public Law 118–49](#)) and by sections 1023(b) and 1023(c) of the POPULIST Act; and

(III) in the determination of the Inspector General, there are any other areas of potential risk or violation; and

(iii) make recommendations to address any deficiencies identified by the Inspector General; and

(B) the Inspector General of the Department of Justice shall assess the information provided by the Department of Justice under subsection (f) of section 603 of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1873](#)), as added by subsection (g) of this section, and include a determination on the accuracy and completeness of the information provided under that section.

(3) Report.—

(A) In general.—For each audit conducted by an Inspector General under paragraph (1), the Inspector General shall submit to the persons specified in subparagraph (B) a report of the audit, including findings and recommendations of the Inspector General and any remediations taken by the Department or element, respectively.

(B) Persons specified.—The persons specified in this subparagraph are the following:

(i) The Attorney General.

(ii) The Director of National Intelligence.

(iii) The Privacy and Civil Liberties Oversight Board.

(iv) The appropriate committees of Congress.

(v) The Foreign Intelligence Surveillance Court (as defined in section 601(e) of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1871\(e\)](#))).

(vi) Any amicus curiae appointed under section 103(i)(2) of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1803\(i\)\(2\)](#)).

(4) Cooperation.—The Attorney General and head of each element of the intelligence community shall ensure full and complete cooperation with the respective Inspector General conducting an audit under paragraph (1), including by providing access to all evidence and information relevant to the assessments required under paragraph (2)(B), subject to such procedures as are necessary to protect the national security of the United States.

(5) Availability to the public.—The Inspector General of each element of the intelligence community shall each make publicly available on a website of the relevant element an unclassified version of any report submitted under paragraph (3) by the respective Inspector General.

(b) Intelligence community parity and communications with Privacy and Civil Liberties Oversight Board.—

(1) Whistleblower protections for members of intelligence community for communications with Privacy and Civil Liberties Oversight Board.—Section 1104 of the National Security Act of 1947 ([50 U.S.C. 3234](#)) is amended—

(A) in subsection (b)(1), in the matter before subparagraph (A), by inserting "the Privacy and Civil Liberties Oversight Board," after "Inspector General of the Intelligence Community,"; and

(B) in subsection (c)(1)(A), in the matter before clause (i), by inserting "the Privacy and Civil Liberties Oversight Board," after "Inspector General of the Intelligence Community,".

(2) Parity in pay for Privacy and Civil Liberties Oversight Board staff and the intelligence community.—Section 1061(j)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004 ([42 U.S.C. 2000ee\(j\)\(1\)](#)) is amended by striking "except that" and all that follows through the period at the end and inserting "except that no rate of pay fixed under this subsection may exceed the highest amount paid by any element of the intelligence community for a comparable position, based on salary information provided to the chairman of the Board by the Director of National Intelligence.".

(c) Congressional oversight of grants of immunity by the Attorney General for warrantless surveillance assistance.—

(1) In general.—[Section 2511\(2\)\(a\) of title 18](#), United States Code, as amended by section 105(d) of this Act, is further amended by adding at the end the following:

"(iv) Not later than 30 days after providing a certification described in clause (B) of the 1st sentence of subparagraph (ii) to a provider of wire or electronic communication service, an officer, employee, or agent thereof, a landlord, a custodian, or another person, the person providing the certification shall submit the certification to the appropriate committees of Congress, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1801](#)).".

(2) Ongoing programs.—

(A) Definitions.—In this paragraph—

(i) the term "appropriate committees of Congress" has the meaning given that term in section 101 of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1801](#)), as amended by this Act;

(ii) the terms "electronic communication", "electronic communication service", and "wire communication" have the meanings given such terms in [section 2510 of title 18](#), United States Code; and

(iii) the term "ongoing certification" means a certification described in clause (B) of the 1st sentence of [section 2511\(2\)\(a\)\(ii\) of title 18](#), United States Code, pursuant to which a provider of wire or electronic communication service, an officer, employee, or agent thereof, a landlord, a custodian, or another person is providing information, facilities, or technical assistance on the date of enactment of this Act.

(B) Submission.—Not later than 90 days after the date of enactment of this Act, the person that provided an ongoing certification to a provider of wire or electronic communication service, an officer, employee, or agent thereof, a landlord, a custodian, or another person shall submit the ongoing certification to the appropriate committees of Congress.

(d) State and local transparency regarding purchased covered personal data.—[Section 2702 of title 18](#), United States Code, as amended by section 105(a) of this Act, is further amended by adding at the end the following:

"(f) Transparency requirements.—

"(1) Definition of covered Federal funds.—In this subsection, the term 'covered Federal funds' means—

"(A) funds provided under the Edward Byrne Memorial Justice Assistance Grant Program under subpart 1 of part E of title I of the Omnibus Crime Control and Safe Streets Act of 1968 ([34 U.S.C. 10151 et seq.](#));

"(B) funds provided through the Office of Community Oriented Policing Services;

"(C) funds received under an in-kind grant made under [section 2576 of title 10](#), United States Code;

"(D) funds received under an in-kind grant made via a transfer made under [section 981 of title 18](#), United States Code; or

"(E) funds received under any other Federal program that offers assistance to a law enforcement agency similar to the assistance under the programs described in subparagraphs (A) through (D).

"(2) Reporting.—If a State or local law enforcement agency, using any means or facility of interstate or foreign commerce, through activities in or affecting interstate or foreign commerce, or by using covered Federal funds, obtains covered personal data in a manner that would violate subsection (e)(2) if obtained by a Federal law enforcement agency in a like manner, the

State or local law enforcement agency shall publicly report, not less frequently than once each year—

"(A) the total amount in dollars of anything of value exchanged for such covered personal data during the preceding year, which shall be disaggregated into money directly exchanged and the estimated value of the other things of value that were exchanged;

"(B) the categories of covered personal data obtained in such a manner in the preceding year, including whether the agency obtained location information, biometric information, web browsing data, or metadata of communications; and

"(C) an estimate of the total number of covered persons whose covered data was obtained in such a manner in the preceding year."

(e) Enhanced annual reports by Director of the Administrative Office of the United States Courts.—Section 603(a)(1) of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1873\(a\)\(1\)](#)) is amended—

(1) in subparagraph (F), by striking "; and" and inserting a semicolon;

(2) in subparagraph (G), by striking the period at the end and inserting a semicolon; and

(3) by adding at the end the following:

"(H) the number of certifications by the Foreign Intelligence Surveillance Court pursuant to section 103(j);

"(I) the number of petitions to certify a question made by an amicus curiae pursuant to section 103(i)(7)(A);

"(J) the number of hearings or rehearings by the Foreign Intelligence Surveillance Court en banc pursuant to section 103(a)(2), disaggregated by hearings or rehearings by such court en banc pursuant to clause (i) or (ii) of such section; and

"(K) the number of times amici curiae have been appointed pursuant to section 103(i)(2)."

(f) Enhanced annual reports by Director of National Intelligence.—

(1) In general.—Subsection (b) of section 603 of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1873\(b\)](#)) is amended—

(A) in paragraph (2)(C), by striking the semicolon and inserting "; and";

(B) by redesignating paragraphs (3) through (7) as paragraphs (6) through (10), respectively;

(C) by inserting after paragraph (2) the following:

"(3) a description of the subject matter of each of the certifications provided under section 702(h);

"(4) statistics revealing the number of persons and identifiers targeted under section 702(a), disaggregated by certification under which the person or identifier was targeted;

"(5) the total number of directives issued pursuant to section 702(i)(1), disaggregated by each type of electronic communication service provider described in each of the subparagraphs of section 701(b)(4);"; and

(D) by adding at the end the following:

"(11) (A) the total number of disseminated intelligence reports derived from collection pursuant to section 702 containing the identities of United States persons regardless of whether the identities of the United States persons were openly included or masked;

"(B) the total number of disseminated intelligence reports derived from collection pursuant to section 702 containing the identities of United States persons in which the identities of the United States persons were masked;

"(C) the total number of disseminated intelligence reports derived from collection outside the authorities provided by this Act containing the identities of United States persons in which the identities of the United States persons were masked;

"(D) the total number of disseminated intelligence reports derived from collection pursuant to section 702 containing the identities of United States persons in which the identities of the United States persons were openly included; and

"(E) the total number of disseminated intelligence reports derived from collection outside the authorities provided by this Act containing the identities of United States persons in which the identities of the United States persons were openly included;

"(12) (A) the number of queries conducted in an effort to find communications or information of or about a covered person that required a warrant pursuant to section 1022(a) of the POPULIST Act; and

"(B) the number of queries conducted in an effort to find communications or information of or about a covered person that did not require a warrant pursuant to section 1022(a) of the POPULIST Act; and

"(13) the number of criminal proceedings in which the Federal Government or a government of a State or political subdivision thereof entered into evidence or otherwise used or disclosed in a criminal proceeding any information obtained or derived from an acquisition conducted for foreign intelligence purposes outside the authorities provided by this Act, regardless of whether such acquisition occurred inside or outside the United States.".

(2) Repeal of nonapplicability to Federal Bureau of Investigation of certain requirements.—Subsection (d) of section 603 of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1873\(d\)](#)) is amended—

(A) by striking paragraph (2); and

(B) by redesignating paragraph (3) as paragraph (2).

(3) Conforming amendment.—Subsection (d)(1) of section 603 of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1873\(d\)\(1\)](#)) is amended by striking "paragraphs (3), (5), or (6)" and inserting "paragraphs (6), (8), or (9)".

(g) Annual reporting on accuracy and completeness of applications.—Section 603 of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1873](#)) is amended—

(1) by redesignating subsections (f) and (g) as subsections (g) and (h), respectively; and

(2) by inserting after subsection (e) the following:

"(f) Annual report by Attorney General on accuracy and completeness of applications.—

"(1) Report required.—In April of each year, the Attorney General shall submit to the appropriate committees of Congress and publish on the website of the Department of Justice, subject to a declassification review, a report setting forth, with respect to the preceding calendar year, the following:

"(A) A summary of all accuracy or completeness reviews of applications for court orders submitted to the Foreign Intelligence Surveillance Court by the Federal Bureau of Investigation under this Act.

"(B) The total number of such applications reviewed for accuracy or completeness.

"(C) The total number of material errors or omissions identified during such reviews.

"(D) The total number of nonmaterial errors or omissions identified during such reviews.

"(E) The total number of instances in which facts contained in an application were not supported by documentation that existed in the applicable file being reviewed at the time of the review.

"(F) An explanation for any increase or decrease in the number of errors identified under subparagraphs (C) and (D), and in the event of an increase in the number of errors, a description of any action taken by the Department of Justice to improve compliance and accuracy.

"(2) Inspector General risk assessment.—In addition to conducting audits under subsection (a) of section 1025 of the POPULIST Act, the Inspector General of the Department of Justice shall—

"(A) periodically assess the reports required by paragraph (1); and

"(B) as determined by the Inspector General, report any risks identified through such assessments to the appropriate committees of Congress.

"(3) Definition of appropriate committees of Congress.—In this subsection, the term 'appropriate committees of Congress' has the meaning given that term in section 101 of this Act."

(h) Allowing more granular aggregate reporting by recipients of foreign intelligence surveillance orders.—Section 604 of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1874](#)) is amended—

(1) in subsection (a)—

(A) by striking paragraphs (1) through (3) and inserting the following:

"(1) A semiannual report that aggregates the number of orders, directives, or national security letters with which the person was required to comply into separate categories of—

"(A) the number of national security letters received, reported—

"(i) for the 1st 1,000 national security letters received, in bands of 200 starting with 1–200; and

"(ii) for more than 1,000 national security letters received, the precise number of national security letters received;

"(B) the number of customer selectors targeted by national security letters, reported—

"(i) for the 1st 1,000 customer selectors targeted, in bands of 200 starting with 1–200; and

"(ii) for more than 1,000 customer selectors targeted, the precise number of customer selectors targeted;

"(C) the number of orders or directives received, combined, under this Act for contents—

"(i) reported—

"(I) for the 1st 1,000 orders and directives received, in bands of 200 starting with 1–200; and

"(II) for more than 1,000 orders and directives received, the precise number of orders and directives received; and

"(ii) disaggregated by whether the order or directive was issued under section 105, 402, or 702;

"(D) the number of customer selectors targeted under orders or directives received, combined, under this Act for contents—

"(i) reported—

"(I) for the 1st 1,000 customer selectors targeted, in bands of 200 starting with 1–200; and

"(II) for more than 1,000 customer selectors targeted, the precise number of customer selectors targeted; and

"(ii) disaggregated by whether the order or directive was issued under section 105, 402, or 702;

"(E) the number of orders or directives received under this Act for noncontents—

"(i) reported—

"(I) for the 1st 1,000 orders or directives received, in bands of 200 starting with 1–200; and

"(II) for more than 1,000 orders or directives received, the precise number of orders and directives received; and

"(ii) disaggregated by whether the order or directive was issued under section 105, 402, or 702; and

"(F) the number of customer selectors targeted under orders or directives under this Act for noncontents—

"(i) reported—

"(I) for the 1st 1,000 customer selectors targeted, in bands of 200 starting with 1–200; and

"(II) for more than 1,000 customer selectors targeted, the precise number of customer selectors targeted; and

"(ii) disaggregated by whether the order or directive was issued under section 105, 402, or 702."; and

(B) by redesignating paragraph (4) as paragraph (2);

(2) by redesignating subsections (b) through (d) as subsections (c) through (e), respectively; and

(3) by inserting after subsection (a) the following:

"(b) Additional disclosures.—A person who publicly reports information under subsection (a) may also publicly report, using a semiannual report, information relating to the previous 180 days that indicates whether the person was or was not required to comply with an order, directive, or national security letter issued under each of sections 105, 402, and 702 and the provisions listed in section 603(g)(3).";

(4) in subsection (c), as redesignated by paragraph (2)—

(A) in paragraph (1), by striking "or (2)";

(B) by striking paragraph (2);

(C) by redesignating paragraph (3) as paragraph (2); and

(D) in paragraph (2), as redesignated by subparagraph (C), by striking "(4)" and inserting "(2)".

(i) Report on use of foreign intelligence surveillance authorities regarding protected activities and protected classes.—

(1) Report.—Not later than July 1, 2027, the Privacy and Civil Liberties Oversight Board shall make publicly available and submit to the appropriate committees of Congress a report on the use of the activities and protected classes described in paragraph (2) in—

(A) applications for orders made by the United States Government under the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1801 et seq.](#)); and

(B) investigations for which such orders are sought.

(2) Activities and protected classes described.—The activities and protected classes described in this paragraph are the following:

(A) Activities and expression protected by the 1st Amendment to the Constitution of the United States.

(B) Race, ethnicity, national origin, and religious affiliation.

(3) Form.—In addition to the report made publicly available and submitted under paragraph (1), the Board may submit to the appropriate committees of Congress a classified annex.

(j) Publication of estimates regarding communications collected under certain provisions of Foreign Intelligence Surveillance Act of 1978.—Not later than 90 days after the date of enactment of this Act, the Director of National Intelligence shall publish a good-faith estimate of—

(1) the number of United States persons whose communications are collected under section 702 of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1881a](#)); or

(2) the number of communications collected under such section to which a party is a person located in the United States at the time of communication.

(k) Enhanced reporting of assessments of compliance with emergency order requirements under certain provisions of the Foreign Intelligence Surveillance Act of 1978.—

(1) Electronic surveillance.—

(A) Annual assessment.—Section 105(e)(6) of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1805\(e\)\(6\)](#)) is amended by striking "shall assess compliance" and inserting "shall not less frequently than annually assess compliance".

(B) Reporting.—Section 108(a)(2) of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1808\(a\)\(2\)](#)) is amended—

(i) in subparagraph (C), by striking "; and" and inserting a semicolon;

(ii) in subparagraph (D), by striking "section 301(e)." and inserting "section 304(e); and"; and

(iii) by adding at the end the following:

"(E) the annual assessment conducted pursuant to section 105(e)(6).".

(2) Physical searches.—

(A) Annual assessment.—Section 304(e)(6) of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1824\(e\)\(6\)](#)) is amended by striking "shall assess compliance" and inserting "shall not less frequently than annually assess compliance".

(B) Reporting.—Section 306 of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1826](#)) is amended—

(i) in paragraph (3), by striking "; and" and inserting a semicolon;

(ii) in paragraph (4), by striking the period and inserting "; and"; and

(iii) by adding at the end the following:

"(5) the annual assessment conducted pursuant to section 304(e)(6).".

SEC. 1026. PROTECTING REPORTERS FROM EXPLOITATIVE STATE SPYING.

(a) Definitions.—In this section:

(1) Covered journalist.—The term "covered journalist" means a person who regularly gathers, prepares, collects, photographs, records, writes, edits, reports, investigates, or publishes news or information that concerns local, national, or international events or other matters of public interest for dissemination to the public.

(2) Covered service provider.—

(A) In general.—The term "covered service provider" means any person that, by an electronic means, stores, processes, or transmits information in order to provide a service to customers of the person.

(B) Inclusions.—The term "covered service provider" includes—

(i) a telecommunications carrier and a provider of an information service (as such terms are defined in section 3 of the Communications Act of 1934 ([47 U.S.C. 153](#)));

(ii) a provider of an interactive computer service and an information content provider (as such terms are defined in section 230 of the Communications Act of 1934 ([47 U.S.C. 230](#)));

(iii) a provider of remote computing service (as defined in [section 2711 of title 18](#), United States Code); and

(iv) a provider of electronic communication service (as defined in [section 2510 of title 18](#), United States Code) to the public.

(3) Document.—The term "document" means writings, recordings, and photographs, as those terms are defined by Federal Rule of Evidence 1001 ([28 U.S.C. App.](#)).

(4) Federal entity.—The term "Federal entity" means an entity or employee of the judicial or executive branch or an administrative agency of the Federal Government with the power to issue a subpoena or issue other compulsory process.

(5) Journalism.—The term "journalism" means gathering, preparing, collecting, photographing, recording, writing, editing, reporting, investigating, or publishing news or information that concerns local, national, or international events or other matters of public interest for dissemination to the public.

(6) Personal account of a covered journalist.—The term "personal account of a covered journalist" means an account with a covered service provider used by a covered journalist that is not provided, administered, or operated by the employer of the covered journalist.

(7) Personal technology device of a covered journalist.—The term "personal technology device of a covered journalist" means a handheld communications device, laptop computer, desktop computer, or other internet-connected device used by a covered journalist that is not provided or administered by the employer of the covered journalist.

(8) Protected information.—The term "protected information" means any information identifying a source who provided information as part of engaging in journalism, and any records, contents of a communication, documents, or information that a covered journalist obtained or created as part of engaging in journalism.

(9) Specified offense against a minor.—The term "specified offense against a minor" has the meaning given that term in section 111(7) of the Adam Walsh Child Protection and Safety Act of 2006 ([34 U.S.C. 20911\(7\)](#)).

(b) Limits on compelled disclosure from covered journalists.—In any matter arising under Federal law, a Federal entity may not compel a covered journalist to disclose protected information, unless a court in the judicial district in which the subpoena or other compulsory process is, or will be, issued determines by a preponderance of the evidence, after providing notice and an opportunity to be heard to the covered journalist, that—

(1) disclosure of the protected information is necessary to prevent, or to identify any perpetrator of, an act of terrorism against the United States; or

(2) disclosure of the protected information is necessary to prevent a threat of imminent violence, significant bodily harm, or death, including specified offenses against a minor.

(c) Limits on compelled disclosure from covered service providers.—

(1) Conditions for compelled disclosure.—In any matter arising under Federal law, a Federal entity may not compel a covered service provider to provide testimony or any document consisting of any record, information, or other communications stored by a covered service provider on behalf of a covered journalist, including testimony or any document relating to a personal account of a covered journalist or a personal technology device of a covered journalist, unless a court in the judicial district in which the subpoena or other compulsory process is, or will be, issued determines by a preponderance of the evidence that there is a reasonable threat of imminent violence unless the testimony or document is provided, and

issues an order authorizing the Federal entity to compel the disclosure of the testimony or document.

(2) Notice to court.—A Federal entity seeking to compel the provision of testimony or any document described in paragraph (1) shall inform the court that the testimony or document relates to a covered journalist.

(3) Notice to covered journalist and opportunity to be heard.—

(A) In general.—A court may authorize a Federal entity to compel the provision of testimony or a document under this subsection only after the Federal entity seeking the testimony or document provides the covered journalist on behalf of whom the testimony or document is stored pursuant to paragraph (1)—

(i) notice of the subpoena or other compulsory request for such testimony or document from the covered service provider not later than the time at which such subpoena or request is issued to the covered service provider; and

(ii) an opportunity to be heard before the court before the time at which the provision of the testimony or document is compelled.

(B) Exception to notice requirement.—

(i) In general.—Notice and an opportunity to be heard under subparagraph (A) may be delayed for not more than 45 days if the court involved determines there is clear and convincing evidence that such notice would pose a clear and substantial threat to the integrity of a criminal investigation, or would present an imminent risk of death or serious bodily harm, including specified offenses against a minor.

(ii) Extensions.—The 45-day period described in clause (i) may be extended by the court for additional periods of not more than 45 days if the court involved makes a new and independent determination that there is clear and convincing evidence that providing notice to the covered journalist would pose a clear and substantial threat to the integrity of a criminal investigation, or would present an imminent risk of death or serious bodily harm, including specified offenses against a minor, under current circumstances.

(d) Limitation on content of information.—The content of any testimony, document, or protected information that is compelled under subsection (b) or (c) shall—

(1) not be overbroad, unreasonable, or oppressive, and, as appropriate, be limited to the purpose of verifying published information or describing any surrounding circumstances relevant to the accuracy of such published information; and

(2) be narrowly tailored in subject matter and period of time covered so as to avoid compelling the production of peripheral, nonessential, or speculative information.

(e) Rule of construction.—Nothing in this section shall be construed to—

(1) apply to civil defamation, slander, or libel claims or defenses under State law, regardless of whether or not such claims or defenses, respectively, are raised in a State or Federal court; or

(2) prevent the Federal Government from pursuing an investigation of a covered journalist or organization that is—

(A) suspected of committing a crime;

(B) a witness to a crime unrelated to engaging in journalism;

(C) suspected of being an agent of a foreign power, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1801](#));

(D) an individual or organization designated under Executive Order 13224 ([50 U.S.C. 1701 note](#); relating to blocking property and prohibiting transactions with persons who commit, threaten to commit, or support terrorism);

(E) a specially designated terrorist, as that term is defined in section 595.311 of title 31, Code of Federal Regulations (or any successor thereto); or

(F) a terrorist organization, as that term is defined in section 212(a)(3)(B)(vi)(II) of the Immigration and Nationality Act ([8 U.S.C. 1182\(a\)\(3\)\(B\)\(vi\)\(II\)](#)).

Subtitle C—Government and Artificial Intelligence

SEC. 1031. FINDINGS AND PURPOSE.

(a) Findings.—Congress finds the following:

(1) Artificial intelligence presents a significant opportunity to improve public administration, expand access to services, strengthen security, support scientific and technical progress, and promote the general welfare of the people of the United States.

(2) Because artificial intelligence can influence decisions affecting rights, liberties, safety, privacy, property, the use of force, and access to essential opportunities and services, the Government bears a special responsibility to ensure that its use of artificial intelligence remains lawful, intelligible, accountable, and subject to meaningful human judgment.

(3) The Federal Government can minimize public dependence on a small number of dominant tech companies and promote competition policy by setting procurement standards that promote interoperability, portability, auditability, and technical independence over opaque and locked systems.

(b) Purpose.—The purpose of this subtitle is to establish public policy for the United States governing artificial intelligence that reflects the highest ideals of the United States, including—

(1) enabling the beneficial use of artificial intelligence to improve public administration, reduce administrative burden, strengthen security, expand access to services, support scientific and technical progress, and help public servants serve the people of the United States more effectively; and