I

119TH CONGRESS
2D SESSION

H. R. 7901

To implement reforms relating to foreign intelligence surveillance authorities, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

MARCH 12, 2026

Mr. DAVIDSON (for himself, Ms. LOFGREN, Ms. JAYAPAL, and Ms. JACOBS) introduced the following bill; which was referred to the Committee on the Judiciary, and in addition to the Permanent Select Committee on Intelligence, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

A BILL

To implement reforms relating to foreign intelligence surveillance authorities, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Government Surveillance Reform Act of 2026''.

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

SEC. 2. DEFINITIONS.

(a) AMENDMENTS 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 such title (50 U.S.C. 1881) is amended by adding at the end the following new paragraph:

''(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.''.

(3) CONFORMING AMENDMENTS.—Such Act (50 U.S.C. 1801 et seq.) is amended—

(A) 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'';

(B) in section 103 (50 U.S.C. 1803)—

(i) 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'';

(ii) in subsection (g)—

(I) in paragraph (2)—

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

(bb) 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'';

(iii) 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'';

(iv) 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 first 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'';

(v) 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'';

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

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

(C) 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'';

(D) 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'";

(E) in section 402 (50 U.S.C. 1842)—

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

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

(F) 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)";

(G) in section 801 (50 U.S.C. 1885)—

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

(ii) by adding at the end the following new paragraph:

"(10) FOREIGN INTELLIGENCE SURVEILLANCE COURT.—The term 'Foreign Intelligence Surveillance

Court' means the court established under section 103(a).''; and

(H) 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''.

(b) TERMS USED IN THIS ACT.—In this Act—

(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 such Act (50 U.S.C. 1881), as amended by subsection (a)(2).

TITLE I—PROTECTIONS FOR UNITED STATES PERSONS WHOSE COMMUNICATIONS ARE COLLECTED UNDER SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

SEC. 101. PROTECTIONS RELATED TO WARRANTLESS QUERIES FOR THE COMMUNICATIONS OF UNITED STATES PERSONS AND PERSONS LOCATED IN THE UNITED STATES.

(a) IN GENERAL.—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 adding at the end the following:

''(7) PROHIBITION ON WARRANTLESS QUERIES FOR THE COMMUNICATIONS AND OTHER INFORMATION OF UNITED STATES PERSONS AND 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 of such approval, a description of the cir-

cumstances 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) is 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.—Each head of an agency who is 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)(7)(F) of such Act, 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 such Act, 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 paragraph (6)—

(A) in the heading, by striking ''NON-UNITED STATES PERSONS'' and inserting ''NON-COVERED PERSONS''; and

(B) by striking ''non-United States persons'' and inserting ''noncovered persons''; and

(3) in paragraphs (1) through (6), by striking ''United States person'' each place it appears and inserting ''covered person''.

SEC. 102. LIMITATION ON USE OF INFORMATION OBTAINED UNDER SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978 RELATING TO UNITED STATES PERSONS AND PERSONS LOCATED IN THE UNITED STATES 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''.

SEC. 103. PROHIBITION ON REVERSE TARGETING OF UNITED STATES PERSONS AND PERSONS LOCATED IN THE UNITED STATES.

Section 702 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881a), as amended by section 101, 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 one 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 that 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 one 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 one 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 one or more particular, known covered persons; and''.

SEC. 104. DATA RETENTION LIMITS FOR INFORMATION COLLECTED UNDER SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

(a) IN GENERAL.—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 a covered person, that has been evaluated and is not specifically known to contain foreign intelligence information; and

''(2) any unevaluated information, unless it can reasonably be determined that the unevaluated information does not contain—

''(A) any information pertaining to a covered person; or

''(B) any communication to or from a covered 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).''.

(b) CLERICAL AMENDMENT.—The table of contents for such Act is amended by inserting after the item relating to section 709 the following:

''Sec. 710. Data retention limits.''.

SEC. 105. FOREIGN INTELLIGENCE SURVEILLANCE COURT SUPERVISION OF DEMANDS FOR TECHNICAL ASSISTANCE FROM ELECTRONIC COMMUNICATION SERVICE PROVIDERS UNDER SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

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 fur-

nished by the provider that has been approved by the Court.''.

SEC. 106. PROHIBITION ON WARRANTLESS ACQUISITION OF DOMESTIC COMMUNICATIONS PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

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''.

SEC. 107. 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''.

SEC. 108. 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.''.

SEC. 109. REPEAL OF EXPANDED DEFINITION OF ELECTRONIC COMMUNICATION SERVICE PROVIDER.

(a) 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—

(1) in subparagraph (F)—

(A) by striking ''custodian,''; and

(B) by striking ''(D), or (E)'' and inserting ''or (D)'';

(2) by striking subparagraph (E);

(3) in subparagraph (D), by striking the semicolon and inserting ''; or''; and

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

(b) DEFINITION WITH RESPECT TO PROTECTION OF PERSONS ASSISTING THE GOVERNMENT.—Section 801(6) of such Act (50 U.S.C. 1885(6)) is amended—

(1) in subparagraph (G)—

(A) by striking ''custodian,''; and

(B) by striking ''(E), or (F)'' and inserting ''or (E)'';

(2) by striking subparagraph (E);

(3) in subparagraph (F), by striking the semicolon and inserting ''; or''; and

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

(c) TREATMENT OF CERTAIN SECTION 702 DIRECTIVES.—Any directive issued pursuant to section 702(i)

of such Act (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 the enactment of this Act, but is not an electronic communication service provider pursuant to such section as in effect after the date of the enactment of this Act, shall be considered null and void.

SEC. 110. REPEAL OF EXPANDED QUERYING REQUIREMENTS FOR PERSONS TRAVELING TO THE UNITED STATES.

Section 702(f) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881a(f)), as amended by section 101, is further amended—

(1) by striking paragraph (6); and

(2) by redesignating paragraph (7), as added by section 101, as paragraph (6).

SEC. 111. FOUR-YEAR EXTENSION OF SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

(a) EXTENSION.—Section 403(b) of the FISA Amendments Act of 2008 (Public Law 110–261) is amended—

(1) in paragraph (1) (50 U.S.C. 1881–1881g note)—

(A) by striking ''effective two years after the date of enactment of the Reforming Intelligence and Securing America Act'' and inserting ''effective April 20, 2030''; and

(B) by striking ''and the Reforming Intelligence and Securing America Act'' and inserting '', the Reforming Intelligence and Securing America Act, and the Government Surveillance Reform Act of 2026''; and

(2) in paragraph (2) (18 U.S.C. 2511 note), in the matter preceding subparagraph (A), by striking ''two years after the date of enactment of the Reforming Intelligence and Securing America Act'' and inserting ''April 20, 2030''.

(b) CONFORMING AMENDMENTS.—Section 404(b) of the FISA Amendments Act of 2008 (Public Law 110–261; 50 U.S.C. 1801 note) is amended—

(1) in paragraph (1)—

(A) in the paragraph heading, by striking ''TWO YEARS AFTER THE DATE OF ENACTMENT OF THE REFORMING INTELLIGENCE AND SECURING AMERICA ACT'' and inserting ''APRIL 20, 2030''; and

(B) by striking ''and the Reforming Intelligence and Securing America Act'' and inserting '', the Reforming Intelligence and Securing America Act, and the Government Surveillance Reform Act of 2026''; and

(2) 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 Government Surveillance Reform Act of 2026''.

TITLE II—FOURTH AMENDMENT IS NOT FOR SALE ACT

SEC. 201. PROHIBITION ON FEDERAL LAW ENFORCEMENT PURCHASE OF PERSONAL DATA FROM DATA BROKERS.

Section 2702 of title 18, United States Code, is amended by adding at the end the following:

''(e) PROHIBITION ON OBTAINING IN EXCHANGE FOR ANYTHING OF VALUE PERSONAL DATA BY FEDERAL LAW ENFORCEMENT AGENCIES.—

''(1) DEFINITIONS.—In this subsection and subsections (f) and (g)—

''(A) the term 'biometric information'—

"(i) means any covered personal data that allows or confirms the unique identification or verification of an individual and is generated from the measurement or processing of unique biological, physical, or physiological characteristics, including—

"(I) fingerprints;

"(II) voice prints;

"(III) iris or retina imagery scans;

"(IV) facial or hand mapping, geometry, or templates; and

"(V) gait; and

"(ii) does not include—

"(I) a digital or physical photograph;

"(II) an audio or video recording; or

"(III) data derived from a digital or physical photograph or an audio or video recording that cannot be used to identify or authenticate a specific individual;

"(B) the term 'covered organization' means a person who—

"(i) is not a governmental entity; and

"(ii) is not an individual, unless such individual is an agent of, or otherwise acting on behalf of, a person who is not a governmental entity and is not an individual;

"(C) the term 'covered person' means an individual who—

"(i) is reasonably believed to be located inside the United States at the time of the creation of the covered personal data; or

"(ii) is a United States person, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801);

"(D) the term 'covered personal data' means personal data relating to a covered person;

"(E) the term 'electronic device' has the meaning given the term 'computer' in section 1030(e);

"(F) the term 'Federal law enforcement agency' means a law enforcement agency of a department or agency of the United States;

"(G) the term 'lawfully obtained public data' means covered personal data obtained by a particular covered organization—

"(i) that the covered organization reasonably understood to have been voluntarily made available to the general public by the covered person;

"(ii) that the covered organization obtained in compliance with all applicable laws and regulations; and

"(iii) if the covered organization did not initially obtain the covered personal data after the covered personal data was made available to the general public—

"(I) that the covered organization reasonably understood to have been obtained in compliance with all applicable laws and regulations by—

"(aa) the person that initially obtained the covered personal data; and

"(bb) if the covered organization did not obtain the covered personal data from the person described in item (aa), each other

person in the sequence of transfers of the covered personal data leading up to the obtaining of the covered personal data by the covered organization; and

''(II) with respect to which the covered organization receives an attestation under penalty of perjury—

''(aa) by the person that initially obtained the covered personal data indicating that the covered personal data was voluntarily made available to the general public by the covered person and was obtained in compliance with all applicable laws and regulations; and

''(bb) if the covered organization did not obtain the covered personal data from the person described in item (aa), by each other person in the sequence of transfers of the covered personal data leading up to the obtaining of the covered personal data by

the covered organization indicating that such person reasonably understood the data to have been lawfully obtained public data;

"(H) the term 'obtain in exchange for anything of value' means to obtain by purchasing, to receive in connection with services being provided for monetary or nonmonetary consideration, or to otherwise obtain in exchange for consideration, including an access fee, service fee, maintenance fee, or licensing fee;

"(I) the term 'personal data'—

"(i) means data, derived data, or any unique identifier that is linked to, or is reasonably linkable to, an individual or to an electronic device that is linked to, or is reasonably linkable to, 1 or more individuals in a household;

"(ii) includes anonymized data that, if combined with other data, can be linked to, or is reasonably linkable to, an individual or to an electronic device that identifies, is linked to, or is reasonably linkable to 1 or more individuals in a household; and

''(iii) does not include data that is lawfully available through Federal, State, or local government records or through widely distributed media; and

''(J) the term 'State or local law enforcement agency' means a law enforcement department or agency of a State, or a political subdivision of a State.

''(2) LIMITATION.—

''(A) IN GENERAL.—

''(i) PROHIBITION.—Subject to clauses (ii) through (vii), a Federal law enforcement agency may not obtain in exchange for anything of value covered personal data if—

''(I) the covered personal data is directly or indirectly obtained from a covered organization; or

''(II) the covered personal data is derived from covered personal data that was directly or indirectly obtained from a covered organization.

''(ii) EXCEPTION FOR CERTAIN COMPILATIONS OF DATA.—A Federal law enforcement agency may obtain in exchange

for something of value covered personal data as part of a larger compilation of data which includes personal data about persons who are not covered persons, if—

"(I) the Federal law enforcement agency is unable through reasonable means to exclude covered personal data from the larger compilation obtained; and

"(II) the Federal law enforcement agency minimizes any covered personal data from the larger compilation, in accordance with the requirements described in, and the procedures established under, subsection (f).

"(iii) EXCEPTION FOR WHISTLEBLOWER DISCLOSURES TO LAW ENFORCEMENT.—Clause (i) shall not apply to covered personal data that is obtained by a Federal law enforcement agency under a program established by an Act of Congress under which a portion of a penalty or a similar payment or bounty is paid to an individual who discloses information about

an unlawful activity to the Government, such as the program authorized under section 7623 of the Internal Revenue Code of 1986 (relating to awards to whistleblowers in cases of underpayments or fraud).

''(iv) EXCEPTION FOR COST REIMBURSEMENT UNDER COMPULSORY LEGAL PROCESS.—Clause (i) shall not apply to covered personal data that is obtained by a Federal law enforcement agency from a covered organization in accordance with compulsory legal process that—

''(I) is established by statute; and

''(II) provides for the reimbursement of costs of the covered organization that are incurred in connection with providing the record or information to the Federal law enforcement agency, such as the reimbursement of costs under section 2706.

''(v) EXCEPTION FOR EMPLOYMENT-RELATED USE.—Clause (i) shall not apply to covered personal data about an employee of, or applicant for employment by,

a Federal law enforcement agency that is—

"(I) obtained by the Federal law enforcement agency for lawful employment-related purposes;

"(II) accessed and used by the Federal law enforcement agency only for such employment-related purposes; and

"(III) destroyed at such time as the covered personal data is no longer needed for employment-related purposes.

"(vi) EXCEPTION FOR USE IN BACKGROUND CHECKS.—Clause (i) shall not apply to covered personal data about a covered person that is—

"(I) obtained by a Federal law enforcement agency for purposes of conducting a background check of the covered person with the written consent of the covered person;

"(II) accessed and used by the Federal law enforcement agency only

for background check-related purposes; and

"(III) destroyed at such time as the covered personal data is no longer needed for background check-related purposes.

"(vii) EXCEPTION FOR LAWFULLY OBTAINED PUBLIC DATA.—

"(I) IN GENERAL.—Except as provided in subclause (II) or (III) of this clause, clause (i) shall not apply to covered personal data that is obtained by a Federal law enforcement agency if—

"(aa) the Federal law enforcement agency reasonably believes that—

"(AA) the covered personal data is lawfully obtained public data; or

"(BB) the covered personal data is derived from covered personal data that solely consists of lawfully obtained public data; and

"(bb) the Federal law enforcement agency receives—

"(AA) an attestation under penalty of perjury from the person providing the covered personal data that the covered personal data is lawfully obtained public data or is derived from covered personal data that solely consists of lawfully obtained public data; and

"(BB) each attestation described in paragraph (1)(G)(iii) with respect to the lawfully obtained public data.

"(II) EXCEPTION FOR BIOMETRIC INFORMATION.—The exception under subclause (I) shall not apply to biometric information.

"(III) EXCEPTION FOR LOCATION INFORMATION.—The exception under

subclause (I) shall not apply to location information.

"(B) INDIRECTLY ACQUIRED RECORDS AND INFORMATION.—The limitation under subparagraph (A) shall apply without regard to whether the covered organization possessing the covered personal data is the covered organization that initially obtained, collected, or received the disclosure of the covered personal data.

"(3) LIMIT ON SHARING BETWEEN AGENCIES.—

"(A) IN GENERAL.—-A Federal law enforcement agency may not acquire, receive, query, or otherwise obtain or access covered personal data from any governmental entity (without regard to whether the governmental entity is a Federal entity), if the covered personal data was obtained by that governmental entity in a manner that would violate paragraph (2) if the Federal law enforcement agency directly obtained the covered personal data in a like manner.

"(B) CAUSATION NOT REQUIRED.—-The prohibition in subparagraph (A) shall apply without regard to whether the Federal law en-

forcement agency caused the governmental entity to obtain the covered personal data.

''(C) ATTESTATION REQUIRED.—-A Federal law enforcement agency may only acquire, receive, query, or otherwise obtain or access covered personal data from another governmental entity (without regard to whether the governmental entity is a Federal entity), if the Federal law enforcement agency obtains an attestation that the covered personal data was not obtained by that governmental entity in a manner that would violate paragraph (2) if the Federal law enforcement agency directly obtained the covered personal data in a like manner.

''(D) DESTRUCTION UPON ACQUISITION OF KNOWLEDGE.—-If a Federal law enforcement agency learns that the Federal law enforcement agency previously acquired, received, queried, or otherwise obtained or accessed covered personal data from any governmental entity (without regard to whether the governmental entity is a Federal entity) that the governmental entity obtained in a manner described in subparagraph (A), the Federal law enforcement agency may not use or disseminate the covered personal

data or any information derived from the covered personal data, and shall promptly destroy any such covered personal data that is still retained.

"(4) PROHIBITION ON USE AS EVIDENCE BY FEDERAL LAW ENFORCEMENT AGENCIES.—

"(A) IN GENERAL.—Covered personal data acquired, received, queried, or otherwise obtained or accessed by a Federal law enforcement agency in violation of paragraph (2) or (3), and any evidence derived therefrom, may not be used, received in evidence, or otherwise disseminated by, on behalf of, or upon a motion or other action by a Federal law enforcement agency in any investigation, trial, hearing, or other proceeding by, in, or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof.

"(B) USE BY AGGRIEVED PARTIES.—Nothing in subparagraph (A) shall be construed to limit the use of covered personal data by a covered person aggrieved of a violation of para-

graph (2) or (3) in connection with any action relating to such a violation.

''(f) MINIMIZATION PROCEDURES.—

''(1) ADOPTION.—

''(A) IN GENERAL.—The Attorney General shall adopt specific procedures that are reasonably designed to minimize the acquisition and retention, and to restrict the querying, of covered personal data, and prohibit the dissemination of information derived from covered personal data, which shall include procedures to enforce the requirements of paragraphs (2), (3), and (4).

''(B) PERIODIC REVIEW.—Not later than 3 years after the date of enactment of the Government Surveillance Reform Act of 2026, and every 3 years thereafter, the Attorney General shall—

''(i) review the procedures adopted under subparagraph (A);

''(ii) publish a determination regarding whether the procedures need to be revised, in light of new technologies or violations of the procedures; and

''(iii) adopt any necessary revisions to the procedures.

''(2) ACQUISITION AND RETENTION.—Each Federal law enforcement agency shall—

''(A) exhaust all reasonable means—

''(i) to exclude covered personal data that is not subject to 1 or more of the exceptions set forth in clauses (iii) through (vii) of subsection (e)(2)(A) from the data obtained; and

''(ii) to remove and delete covered personal data described in clause (i) after a compilation is obtained and before operational use of the compilation or inclusion of the compilation in a dataset intended for operational use; and

''(B) audit the acquisition and retention of covered personal data by the Federal law enforcement agency on an ongoing and continuous basis, to evaluate compliance with the procedures adopted under paragraph (1).

''(3) DESTRUCTION.—If a Federal law enforcement agency identifies covered personal data in a compilation described in paragraph (2)(A)(ii), the Federal law enforcement agency shall promptly de-

stroy the covered personal data and any dissemination of information derived from the covered personal data shall be prohibited.

''(4) QUERYING.—

''(A) IN GENERAL.—Except as provided in subparagraphs (B) and (C), no officer or employee of a Federal law enforcement agency may conduct a query of personal data, including personal data already subjected to minimization, in an effort to find records of or about 1 or more particular covered persons.

''(B) EXCEPTIONS.—Subparagraph (A) shall not apply to a query related to 1 or more particular covered persons if—

''(i) such covered persons are the subject of a court order issued under this title or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) that would authorize the Federal law enforcement agency to compel the production of the covered personal data, during the effective period of that order;

''(ii) the officer or employee of a Federal law enforcement agency carrying out the query has a reasonable belief that the

life or safety of such covered persons are threatened and the information is sought for the purpose of assisting such covered persons, in which case information resulting from the query may be accessed or used solely for that purpose and shall be destroyed at such time as it is no longer necessary for such purpose; or

''(iii) such covered persons have consented to the query.

''(C) SPECIAL RULE FOR COMPILATIONS OF DATA.—For a query of a compilation of data obtained under subsection (e)(2)(A)(ii)—

''(i) each query shall be reasonably designed to exclude personal data of covered persons; and

''(ii) any personal data of covered persons returned pursuant to a query shall not be reviewed and shall immediately be destroyed.

''(g) 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;

"(D) funds received under an in-kind grant made via a transfer made under section 981 of this title; 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 en-

forcement agency shall publicly report, not less frequently than once per 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.".

TITLE III—ADDITIONAL REFORMS RELATING TO ACTIVITIES UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

SEC. 301. COURT SUPERVISION OF COLLECTION TARGETING UNITED STATES PERSONS AND PERSONS LOCATED INSIDE THE UNITED STATES.

(a) IN GENERAL.—Title VII of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881 et seq.) is amended—

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

(2) by inserting after section 702 (50 U.S.C. 1881a) the following:

"SEC. 703. ACQUISITIONS TARGETING UNITED STATES 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) PEN REGISTER OR TRAP AND TRACE.—No officer or employee of the Federal Government may intentionally target a covered person for the purpose of collecting foreign intelligence information through the installation and use of a pen register or trap and trace device, or to acquire information the compelled production of which would require a pen register or trap and trace device

order if conducted inside the United States, unless such person is the subject of—

''(1) an order or emergency authorization under title IV 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 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 installation and use of a pen register or trap and trace device pursuant to section 105(e), 304(e), or 403(a) of this Act is denied, or in any other case in which the acquisition has been conducted and no order is issued approving the acquisition—

''(1) no information obtained or evidence derived from such acquisition 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 obtained or evidence derived from such acquisition concerning a covered person 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.''.

(b) CONFORMING AMENDMENTS.—The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is further amended—

(1) in section 601(a)(1) (50 U.S.C. 1871(a)(1))—

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

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

(2) 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

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

(c) CLERICAL AMENDMENT.—The table of contents for such Act is amended—

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

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

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

SEC. 302. CONSISTENT DISCLOSURES OF RELEVANT INFORMATION IN TITLE V AND OTHER FISA APPLICATIONS.

(a) 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), are amended by inserting '', and that the application fairly reflects all information,'' after ''apprised of all information'' each place it appears.

(b) TECHNICAL CORRECTIONS.—Such Act is further amended—

(1) in section 104(a)—

(A) in paragraph (9), by striking ''; and'' and inserting a semicolon;

(B) in paragraph (11), by striking ''; and'' and inserting a semicolon; and

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

(2) in section 303(a)—

(A) in paragraph (9), by striking ''; and'' and inserting a semicolon; and

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

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

SEC. 303. STRENGTHENING ACCURACY PROCEDURES.

(a) 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 and auditing mechanisms on an annual basis to assess the efficacy of the accuracy procedures that have been adopted and reports such findings to the Attorney General.

''(b) STATEMENT AND CERTIFICATION OF ACCURACY PROCEDURES.—Any Federal officer or employee making an application for a court order under this Act shall include with the application—

''(1) a description of the accuracy procedures employed by the officer or employee, or their designee; and

''(2) a certification that the officer or employee, or their designee, has collected and reviewed for accuracy and completeness—

''(A) supporting documentation for each factual assertion contained in the application;

''(B) 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; and

''(C) all material information that might reasonably call into question the reliability and reporting of any information from any confidential human source that is used in the application.

''(c) NECESSARY FINDING FOR COURT ORDERS.—A judge may not enter an order under this Act unless the judge finds, in addition to any other findings required under this Act, that the accuracy procedures described in the application for the order, as required under subsection (b)(1), are actually accuracy procedures as defined in this section.''.

(b) 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.".

(c) TIMELINE TO ADOPT NEW ACCURACY PROCEDURES.—

(1) IN GENERAL.—Not later than 180 days after the date of the 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 subsection (a)).

(2) REPEAL OF ACCURACY PROCEDURES REQUIREMENT FROM RISAA.—On the day that is 180 days after the date of the 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.

SEC. 304. CLARIFICATION REGARDING TREATMENT OF INFORMATION AND EVIDENCE ACQUIRED UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

(a) IN GENERAL.—Section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801), as amended by section 2(a), 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.''.

(b) POLICIES AND GUIDANCE.—

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

(A) Policies concerning the application of subsection (t) of section 101 of such Act, as added by subsection (a).

(B) 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 en-

forcement responsibilities concerning the application of such subsection (t).

(2) MODIFICATIONS.—Whenever the Attorney General and the Director modify a policy or guidance published under paragraph (1), the Attorney General and the Director shall publish such modifications.

SEC. 305. 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 the enactment of the Government Surveillance Reform Act of 2026'' after ''continue in effect''.

SEC. 306. 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.''.

SEC. 307. APPOINTMENT OF AMICI CURIAE AND ACCESS TO INFORMATION.

(a) EXPANSION OF APPOINTMENT AUTHORITY.—

(1) IN GENERAL.—Section 103(i)(2) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(i)(2)) is amended—

(A) in subparagraph (A)—

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

''(i) shall appoint one or more individuals who have been designated under paragraph (1) and who possesses 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 appoint-

ment 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);

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

''(ii) shall appoint one or more individuals who have been designated under paragraph (1) and who possesses 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 ap-

proval 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

(B) by striking subparagraph (B).

(2) DEFINITION OF SENSITIVE INVESTIGATIVE MATTER.—Section 103(i) of such Act (50 U.S.C. 1803(i)) is amended 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).''.

(3) QUALIFICATIONS.—Section 103(i)(3)(A) of such Act (50 U.S.C. 1803(i)(3)(A)) is amended—

(A) by inserting ''cybersecurity, cryptography,'' after ''communications technology,''; and

(B) by adding at the end the following: ''Of such individuals, at least one shall possess

legal expertise and at least one shall possess technical expertise.''.

(4) NOTIFICATION.—Section 103(i) of such Act (50 U.S.C. 1803(i)) is amended by striking paragraph (7) and inserting the following:

''(7) NOTIFICATION.—The presiding judge of the Foreign Intelligence Surveillance Court and the Foreign Intelligence Surveillance Court or 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).''.

(5) SECTION 702 RECERTIFICATION SCHEDULE.—Section 702(j)(5)(A) of such Act (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).''.

(b) AUTHORITY TO SEEK REVIEW.—Section 103(i) of such Act (50 U.S.C. 1803(i)), as amended by subsection (a), is further amended—

(1) in paragraph (4)—

(A) in the paragraph heading, by inserting ''; AUTHORITY'' after ''DUTIES'';

(B) in the matter preceding subparagraph (A), by striking ''shall'';

(C) 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 the following: '', 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'';

(D) by striking subparagraph (A);

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

(F) 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.'';

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

(3) 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).''.

(c) ACCESS TO INFORMATION.—

(1) APPLICATION AND MATERIALS.—Section 103(i)(6) of such Act (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 prece-

dent 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 902.''.

(2) CLARIFICATION OF ACCESS TO CERTAIN INFORMATION.—Section 103(i)(6) of such Act (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 in-

formation, any classified documents, information, and other materials or proceedings.''.

(3) CONSULTATION AMONG AMICI CURIAE.—Section 103(i)(6) of such Act (50 U.S.C. 1803(i)(6)), as amended by paragraphs (1) and (2), 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 one 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.''.

SEC. 308. DECLASSIFICATION OF SIGNIFICANT DECISIONS, ORDERS, AND OPINIONS.

Section 602 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1872) is amended by striking subsection (a) and inserting the following:

''(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) complete the declassification review required by subparagraph (A) and public release of each such decision, order, or opinion pursuant to subparagraph (B) 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 the 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)(12)); or

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

SEC. 309. CLARIFICATION OF FOREIGN INTELLIGENCE SURVEILLANCE COURT JURISDICTION OVER RECORDS OF THE COURT AND OTHER ANCILLARY MATTERS.

(a) IN GENERAL.—Section 103 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803), as amended by sections 206 and 207, is further amended—

(1) 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.'';

(2) 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

(3) in subsection (k)(1), by striking ''section 1254(2) of title 28'' and inserting ''section 1254 of title 28''.

(b) TECHNICAL CORRECTIONS.—Section 103 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803), as amended by section (a), is further amended—

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

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

SEC. 310. 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.

(a) IN GENERAL.—The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), as amended by section 202, is further amended by adding at the end the following:

"TITLE X—ADDITIONAL MATTERS

"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.''.

(b) CLERICAL AMENDMENT.—The table of contents of the Foreign Intelligence Surveillance Act of 1978, as amended by section 202, is further amended by adding at the end the following:

''TITLE X—ADDITIONAL MATTERS

''Sec. 1001. Challenges to Government surveillance.''.

SEC. 311. ACCOUNTABILITY PROCEDURES FOR VIOLATIONS BY FEDERAL EMPLOYEES.

(a) IN GENERAL.—Title X of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881 et seq.), as added by section 310, is amended by adding at the end the following:

''SEC. 1002. ACCOUNTABILITY PROCEDURES FOR VIOLATIONS BY FEDERAL EMPLOYEES.

''(a) DEFINITIONS.—In this section:

''(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term 'appropriate committees of Con-

gress' 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 Government Surveillance Reform Act of 2026, 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 second 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 third 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 second 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 third reckless or negligent violation under subparagraph (C)(ii) of subsection (c)(2) or a second 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.''.

(b) CLERICAL AMENDMENT.—The table of contents for such Act is amended by inserting after the item relating to section 1001, as added by section 310, the following:

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

(c) REPORT REQUIRED.—

(1) IN GENERAL.—Not later than 180 days after the date of the 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 subsection (a)), shall submit to the appropriate committees of Congress a report detailing—

(A) the procedures established under section 1002 of the Foreign Intelligence Surveillance Act of 1978, as added by subsection (a); and

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

(2) FORM.—The report required by paragraph (1) shall be submitted in unclassified form, but may include a classified annex to the extent necessary to protect sources and methods.

(d) DECONFLICTION WITH RISAA ACCOUNTABILITY PROCEDURES.—

(1) IN GENERAL.—Paragraph (4) of section 702(f) of such Act (50 U.S.C. 1881a(f)) is repealed.

(2) CONFORMING AMENDMENT.—Paragraph (6) of such section 702(f), as added by section 101 and redesignated by section 110, is redesignated as paragraph (4) and moved before paragraph (5) of such section 702(f).

(3) EFFECT DATE.—The amendments made by paragraphs (1) and (2) shall take effect on the date that is 180 days after the date of the enactment of this Act.

SEC. 312. REFORMS TO THE EXCLUSIVE MEANS LIMITATIONS UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

(a) CHAPTER 119 OF TITLE 18.—Section 2511(2)(f) of title 18, United States Code, is amended to read as follows:

''(f)(i) Other than as provided in subsection (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.''.

(b) FOREIGN INTELLIGENCE SURVEILLANCE ACT.—Section 112 of the Foreign Intelligence Surveillance Act (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 title IV of the Government Surveillance Reform 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.''.

TITLE IV—REFORMS RELATED TO SURVEILLANCE CONDUCTED FOR FOREIGN INTELLIGENCE PURPOSES OTHER THAN UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

SEC. 401. DEFINITIONS.

In this title:

(1) CONGRESSIONAL INTELLIGENCE COMMITTEES, INTELLIGENCE, INTELLIGENCE COMMUNITY, AND FOREIGN INTELLIGENCE.—The terms ''congressional intelligence committees'', ''intelligence'', ''intelligence community'', and ''foreign intelligence'' have the meanings given such terms in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

(2) ELECTRONIC SURVEILLANCE, PERSON, STATE, UNITED STATES, AND UNITED STATES PERSON.—The terms ''electronic surveillance'', ''per-

son'', ''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).

SEC. 402. PROTECTIONS RELATED TO WARRANTLESS QUERIES FOR THE COMMUNICATIONS OF UNITED STATES PERSONS AND PERSONS LOCATED IN THE UNITED STATES.

(a) DEFINITIONS.—In this section:

(1) COVERED INFORMATION.—The term ''covered information'' includes—

(A) communications content; and

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

(2) COVERED QUERY.—The term ''covered query'' means a query—

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

(B) for a significant purpose of retrieving information of, or concerning 1 or more covered persons.

(3) QUERY.—

(A) IN GENERAL.—The term ''query'' means the use of 1 or more terms, whether conducted through manual or automated means, to retrieve any information described in subparagraph (B), including retrieval from a subset of such information, whether that subset was created by retrieval through a query or other means.

(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.

(b) IN GENERAL.—Except as provided in subsections (c) and (d), no officer or employee of the Federal Government may access covered information returned in response to a covered query.

(c) EXCEPTIONS FOR CONCURRENT AUTHORIZATION, CONSENT, EMERGENCY SITUATIONS, AND CERTAIN DEFENSIVE CYBERSECURITY QUERIES.—Subsection (b) shall not apply if—

(1) 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—

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

(B) 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;

(2)(A) 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 clause (i), the query must be conducted before authorization described in subparagraph (A) can, with due diligence, be obtained; and

(B) 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;

(3) 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

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

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

(C) 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.

(d) MATTERS RELATING TO EMERGENCY QUERIES.—

(1) TREATMENT OF DENIALS.—If covered information is accessed pursuant to an emergency au-

thorization described in subsection (c)(1) 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 section—

(A) 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

(B) 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.

(2) ASSESSMENT OF COMPLIANCE.—Not less frequently than annually, the Attorney General shall assess compliance with the requirements under paragraph (1).

(e) FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.—This section 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.).

(f) FOREIGN INTELLIGENCE PURPOSE REQUIRED FOR QUERIES.—

(1) IN GENERAL.—Except as provided in paragraph (2), no officer or employee of the Federal Government may conduct a query unless the query is—

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

(B) made with a significant foreign intelligence purpose.

(2) 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, as amended by section 101, applies.

(g) 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—

(1) for each query—

(A) each term used for the conduct of the query;

(B) the date of the covered query;

(C) the identifier of the officer or employee who conducted the covered query;

(D) a statement of facts justifying that it is reasonably likely to retrieve foreign intelligence information or an exception under subsection (f)(2) applies; and

(E) a description of the basis for the exception; and

(2) for each access—

(A) the date of the access;

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

(C) a statement of facts showing that an access is authorized by an exception under subsection (c).

(h) QUERY RECORD SYSTEM.—

(1) 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 subsection (g), 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.

(2) COMPLIANCE REPORT.—Not later than 90 days after the date of the enactment of this Act, the head of each applicable agency shall report to the congressional intelligence committees on its compliance with paragraph (1).

SEC. 403. PROHIBITION ON REVERSE TARGETING OF UNITED STATES PERSONS AND PERSONS LOCATED IN THE UNITED STATES.

(a) PROHIBITION ON ACQUISITION.—No officer or employee of the Federal Government may intentionally target, for the purpose of acquiring foreign intelligence in-

formation, 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—

(1)(A) 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;

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

(C) 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

(2) 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.

(b) FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978 AND CRIMINAL WARRANTS.—This section shall not apply to—

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

(2) 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.

SEC. 404. PROHIBITION ON INTELLIGENCE ACQUISITION OF UNITED STATES PERSON DATA.

(a) COVERED DATA DEFINED.—In this section, the term ''covered data'' means—

(1) 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;

(2) 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

(3) does not include data that—

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

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

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

(b) LIMITATION.—

(1) IN GENERAL.—Subject to paragraphs (2) through (8), an element of the intelligence community may not acquire a dataset that includes covered data.

(2) 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.

(3) 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—

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

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

(4) 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—

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

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

(5) EXCEPTION FOR LIFE OR SAFETY.—An element of the intelligence community may acquire covered data if—

(A) there is 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 this threat, the acquisition must be conducted before authorization pursuant to paragraph (2) can, with due diligence, be obtained;

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

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

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

(6) EXCEPTION FOR CONSENT.—An element of the intelligence community may acquire covered data if—

(A) 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;

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

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

(7) 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 subsection (c).

(8) 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—

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

(B) 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

(C) 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.

(c) MINIMIZATION PROCEDURES.—

(1) 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 subsection (b).

(2) ACQUISITION AND RETENTION.—The procedures adopted under paragraph (1) shall require elements of the intelligence community to exhaust all reasonable means—

(A) to exclude covered data not subject to 1 or more exceptions set forth in subsection (b) from datasets prior to acquisition; and

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

(3) DESTRUCTION.—The procedures adopted under paragraph (1) shall require that if an element of the intelligence community identifies covered data acquired in violation of subsection (b), such covered data shall be promptly destroyed.

(d) PROHIBITION ON USE OF DATA OBTAINED IN VIOLATION OF THIS SECTION.—Covered data acquired by an element of the intelligence community in violation of

subsection (b), 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.

(e) REPORTING REQUIREMENT.—

(1) IN GENERAL.—Not later than 180 days after the date of the 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 section.

(2) CONTENTS.—The report submitted pursuant to paragraph (1) shall include the following:

(A) 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;

(B) DATA COLLECTION.—A description of data collected pursuant to subsection (b)(8), 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.

(C) DETECTED VIOLATIONS.—A description of covered data identified as having been acquired in violation of subsection (b) in the preceding year, including—

(i) an estimate of the number of covered persons whose information was acquired in violation of subsection (b); and

(ii) any changes made to the procedures in subsection (c) to address compliance issues.

(3) NOTIFICATIONS.—After submitting the report required by paragraph (1), the Director shall, in coordination with the Under Secretary, notify the

appropriate committees of Congress of any changes to the information contained in such report.

(4) AVAILABILITY TO THE PUBLIC.—The Director shall make available to the public on the website of the Director—

(A) the unclassified portion of the report submitted pursuant to paragraph (1); and

(B) any notifications submitted pursuant to paragraph (3).

(f) RULE OF CONSTRUCTION.—Nothing in this section 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.

SEC. 405. 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.

SEC. 406. DATA RETENTION LIMITS.

(a) PROCEDURES.—

(1) IN GENERAL.—Each head of an element of the intelligence community shall develop and implement procedures governing the retention of information described in paragraph (2).

(2) INFORMATION DESCRIBED.—The information described in this paragraph 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.

(b) REQUIREMENTS.—

(1) COVERED INFORMATION DEFINED.—In this subsection, the term ''covered information'' includes—

(A) 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

(B) 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.

(2) IN GENERAL.—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—

(A) 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

(B) 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)).

SEC. 407. 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 the enactment of the Government Surveillance Reform Act of 2026, such report shall be made publicly available pursuant to paragraph (1) by not later than 180 days after the date of the enactment of such 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.).''.

TITLE V—INDEPENDENT OVERSIGHT

SEC. 501. INSPECTOR GENERAL OVERSIGHT OF ORDERS UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

(a) AUDIT.—Not later than 1 year after the date of the enactment of this Act, 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.

(b) SCOPE; CONTENTS.—In conducting an audit under subsection (a)—

(1) an Inspector General shall—

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

(B) 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 made by sections 302 and 303 of this Act; and

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

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

(2) 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 section 803 of this Act, and include a determination on the accuracy and completeness of the information provided under that section.

(c) REPORT.—

(1) IN GENERAL.—For each audit conducted by an Inspector General under subsection (a), such Inspector General shall submit to the persons specified in paragraph (2) a report of the audit, including findings and recommendations of the Inspector General and any remediations taken by the Department or element, respectively.

(2) PERSONS SPECIFIED.—The persons specified in this paragraph are the following:

(A) The Attorney General.

(B) The Director of National Intelligence.

(C) The Privacy and Civil Liberties Oversight Board.

(D) The appropriate committees of Congress.

(E) 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))).

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

(d) 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 subsection (a), including by providing access to all evidence and information relevant to the assessments required under subsection (b)(2), subject to such procedures as are necessary to protect the national security of the United States.

(e) 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 sub-

mitted under subsection (c) by the respective Inspector General.

SEC. 502. INTELLIGENCE COMMUNITY PARITY AND COMMUNICATIONS WITH PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD.

(a) 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—

(1) 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

(2) 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,''.

(b) 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 sub-

section 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.''.

SEC. 503. CONGRESSIONAL OVERSIGHT OF GRANTS OF IMMUNITY BY THE ATTORNEY GENERAL FOR WARRANTLESS SURVEILLANCE ASSISTANCE.

(a) IN GENERAL.—Section 2511(2)(a) of title 18, United States Code, is amended by adding at the end the following:

''(iv) Not later than 30 days after providing a certification described in clause (B) of the first 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).''.

(b) ONGOING PROGRAMS.—

(1) DEFINITIONS.—In this subsection—

(A) the term ''appropriate committees of Congress'' has the meaning given that term in section 101 of the Foreign Intelligence Surveil-

lance Act of 1978 (50 U.S.C. 1801), as amended by section 2 of this Act;

(B) 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

(C) the term ''ongoing certification'' means a certification described in clause (B) of the first 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.

(2) 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.

TITLE VI—REFORMS TO THE ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986

SEC. 601. WARRANT PROTECTIONS FOR LOCATION INFORMATION, WEB BROWSING RECORDS, AND SEARCH QUERY RECORDS.

(a) HISTORICAL LOCATION, WEB BROWSING, AND SEARCH QUERIES.—

(1) IN GENERAL.—Section 2703 of title 18, United States Code, is amended—

(A) in subsection (a)—

(i) in the subsection heading, by striking ''CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS'' and inserting ''LOCATION INFORMATION, WEB BROWSING RECORDS, SEARCH QUERY RECORDS, OR CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS''; and

(ii) in the first sentence, by inserting ''location information, a web browsing record, a search query record, or'' before ''the contents of a wire''; and

(B) in subsection (c)(1), in the matter preceding subparagraph (A), by inserting ''location

information, a web browsing record, a search query record, or'' before ''the contents''.

(2) DEFINITION.—Section 2711 of title 18, United States Code, is amended—

(A) in the matter preceding paragraph (1), by inserting ''(a) IN GENERAL.—'' before ''As used'';

(B) in subsection (a), as so designated—

(i) in paragraph (3)(C), by striking ''and'' at the end;

(ii) in paragraph (4), by striking the period at the end and inserting a semicolon; and

(iii) by adding at the end the following:

''(5) the term 'location information' means information derived or otherwise calculated from the transmission or reception of a radio signal that reveals the approximate or actual geographic location of a customer, subscriber, user, or device;

''(6) the term 'web browsing record'—

''(A) means a record that reveals, in part or in whole, the identity of a service provided by an online service provider, or the identity of a customer, subscriber, user, or device, for any

attempted or successful communication or transmission between an online service provider and such a customer, subscriber, user, or device;

''(B) includes a record that reveals, in part or in whole—

''(i) the domain name, uniform resource locator, internet protocol address, or other identifier for a service provided by an online service provider with which a customer, subscriber, user, or device has exchanged or attempted to exchange a communication or transmission; or

''(ii) the network traffic generated by an attempted or successful communication or transmission between a service provided by an online service provider and a customer, subscriber, user, or device; and

''(C) does not include a record that reveals information about an attempted or successful communication or transmission between a known service and a particular known customer, subscriber, user, or device, if the record is maintained by the known service and is limited to revealing additional identifying informa-

tion about the particular known customer, subscriber, user, or device; and

''(7) the term 'search query record'—

''(A) means a record that reveals a query term or instruction submitted, in written, verbal, or other format, by a customer, subscriber, user, or device to any service provided by an online service provider, including a search engine, voice assistant, chat bot, or navigation service; and

''(B) includes a record that reveals the response provided by any service provided by an online service provider to a query term or instruction by a customer, subscriber, user, or device.''; and

(C) by adding at the end the following:

''(b) RULE OF CONSTRUCTION.—Nothing in this section or section 2510 shall be construed to mean that a record may not be more than 1 of the following types of record:

''(1) The contents of a communication.

''(2) Location information.

''(3) A web browsing record.

''(4) A search query record.''.

(b) REAL-TIME SURVEILLANCE OF LOCATION INFORMATION.—Section 3117 of title 18, United States Code, is amended—

(1) in the section heading, by striking "**Mobile tracking devices**" and inserting "**Tracking orders for Federal departments and agencies**";

(2) by striking subsection (b);

(3) by redesignating subsection (a) as subsection (c);

(4) by inserting before subsection (c), as so redesignated, the following:

"(a) IN GENERAL.—No officer or employee of a governmental entity may install or direct the installation of a tracking device, except pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures and, in the case of a court-martial or other proceeding under chapter 47 of title 10 (the Uniform Code of Military Justice), issued under section 846 of that title, in accordance with regulations prescribed by the President) by a court of competent jurisdiction.

"(b) EMERGENCIES.—

''(1) IN GENERAL.—Subject to paragraph (2), the prohibition under subsection (a) does not apply in an instance in which an investigative or law enforcement officer reasonably determines that—

''(A) a circumstance described in subparagraph (i), (ii), or (iii) of section 2518(7)(a) exists; and

''(B) there are grounds upon which a warrant could be issued to authorize the installation of the tracking device.

''(2) APPLICATION DEADLINE.—If a tracking device is installed under the authority under paragraph (1), an application for a warrant shall be made within 48 hours after the installation.

''(3) TERMINATION ABSENT WARRANT.—In the absence of a warrant, use of a tracking device under the authority under paragraph (1) shall immediately terminate when the investigative information sought is obtained or when the application for the warrant is denied, whichever is earlier.

''(4) LIMITATION.—In the event an application for a warrant described in paragraph (2) is denied, or in any other case where the use of a tracking device under the authority under paragraph (1) is terminated without a warrant having been issued, the

information obtained shall be treated as having been obtained in violation of this section, and an inventory describing the installation and use of the tracking device shall be served on the person named in the warrant application.'';

(5) in subsection (c), as so redesignated—

(A) in the subsection heading, by striking ''IN GENERAL'' and inserting ''JURISDICTION'';

(B) by striking ''or other order'';

(C) by striking ''mobile'';

(D) by striking ''such order'' and inserting ''such warrant''; and

(E) by adding at the end the following: ''For purposes of this subsection, the installation of a tracking device occurs within the jurisdiction in which the device is physically located when the installation is complete.''; and

(6) by adding at the end the following:

''(d) DEFINITIONS.—As used in this section—

''(1) the term 'computer' has the meaning given that term in section 1030(e);

''(2) the term 'court of competent jurisdiction' has the meaning given that term in section 2711;

''(3) the term 'governmental entity'—

"(A) means a department or agency of the United States; and

"(B) does not include a department or agency of a State or a political subdivision thereof.

"(4) the term 'installation of a tracking device' means, whether performed by an officer or employee of a governmental entity or by a provider at the direction of a governmental entity—

"(A) the physical placement of a tracking device;

"(B) the remote activation of the tracking software or functionality of a tracking device; or

"(C) the acquisition of a radio signal transmitted by a tracking device; and

"(5) the term 'tracking device' means an electronic or mechanical device which permits the tracking of the movement of a person or object, including a phone, wearable device, connected vehicle, or other computer owned, used, or possessed by the target of surveillance.".

(c) PROSPECTIVE SURVEILLANCE OF WEB BROWSING RECORDS AND LOCATION INFORMATION.—Section 2703 of title 18, United States Code, is amended by adding at the end the following:

''(i) PROSPECTIVE DISCLOSURE OF WEB BROWSING RECORDS.—

''(1) IN GENERAL.—A governmental entity may require the prospective disclosure by an online service provider of a web browsing record only pursuant to a warrant issued using the procedures described in subsection (a).

''(2) TIME RESTRICTIONS.—A warrant requiring the prospective disclosure by an online service provider of web browsing records may require disclosure of web browsing records for only a period as is necessary to achieve the objective of the disclosure, not to exceed 30 days from issuance of the warrant. Extensions of such a warrant may be granted, but only upon satisfaction of the showings necessary for issuance of the warrant in the first instance.

''(j) PROSPECTIVE DISCLOSURE OF LOCATION RECORDS.—A governmental entity may require the prospective disclosure by an online service provider of location information only pursuant to a warrant issued using the procedures described in subsection (a), that satisfies the restrictions imposed on warrants for tracking devices imposed by section 3117 of this title and rule 41 of the Federal Rules of Criminal Procedure.''.

SEC. 602. CONSISTENT PROTECTIONS FOR PHONE AND APP-BASED CALL AND TEXTING RECORDS.

Section 2703(c)(2)(C) of title 18, United States Code, is amended by striking ''local and long distance telephone connection records, or''.

SEC. 603. EMAIL PRIVACY ACT.

(a) SHORT TITLE.—This section may be cited as the ''Email Privacy Act''.

(b) VOLUNTARY DISCLOSURE CORRECTIONS.—Section 2702 of title 18, United States Code, is amended—

(1) in subsection (a)—

(A) in paragraph (1)—

(i) by striking ''divulge'' and inserting ''disclose''; and

(ii) by striking ''while in electronic storage by that service'' and inserting ''that is in electronic storage with or otherwise stored, held, or maintained by that service'';

(B) in paragraph (2)—

(i) by striking ''to the public'';

(ii) by striking ''divulge'' and inserting ''disclose''; and

(iii) by striking ''which is carried or maintained on that service'' and inserting

''that is stored, held, or maintained by that service''; and

(C) in paragraph (3)—

(i) by striking ''divulge'' and inserting ''disclose''; and

(ii) by striking ''a provider of'' and inserting ''a person or entity providing'';

(2) in subsection (b)—

(A) in the matter preceding paragraph (1)—

(i) by striking ''divulge'' and inserting ''disclose''; and

(ii) by inserting ''wire or electronic'' before ''communication'';

(B) by amending paragraph (1) to read as follows:

''(1) to an originator, addressee, or intended recipient of such communication, to the subscriber or customer on whose behalf the provider stores, holds, or maintains such communication, or to an agent of such addressee, intended recipient, subscriber, or customer;''; and

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

''(3) with the lawful consent of the originator, addressee, or intended recipient of such communication, or of the subscriber or customer on whose behalf the provider stores, holds, or maintains such communication;''; and

(3) in subsection (c)—

(A) in the matter preceding paragraph (1)—

(i) by striking ''divulge'' and inserting ''disclose''; and

(ii) by inserting ''wire or electronic'' before ''communications''; and

(B) by amending paragraph (2) to read as follows:

''(2) with the lawful consent of the subscriber or customer;''.

(c) AMENDMENTS TO REQUIRED DISCLOSURE SECTION.—Section 2703 of title 18, United States Code, as amended by this Act, is amended—

(1) in subsection (a), in the first sentence—

(A) by striking ''A governmental entity'' and inserting ''Except as provided in subsections (l) and (m), a governmental entity'';

(B) by striking ''pursuant to'' and inserting ''if the governmental entity obtains''; and

(C) by striking ''by a court of competent jurisdiction.'' and inserting ''that is issued by a court of competent jurisdiction and that may indicate the date by which the provider must make the disclosure to the governmental entity. In the absence of a date on the warrant indicating the date by which the provider must make disclosure to the governmental entity, the provider shall promptly respond to the warrant.'';

(2) in subsection (c)—

(A) in paragraph (1)—

(i) in the matter preceding subparagraph (A)—

(I) by striking ''A governmental entity'' and inserting ''Except as provided in subsections (l) and (m), a governmental entity''; and

(II) by striking ''only when the governmental entity—'' and inserting ''only—'';

(ii) in subparagraph (A)—

(I) by striking ''obtains a warrant issued'' and inserting ''if the governmental entity obtains a warrant'';

(II) by striking ''by the President) by a court'' and inserting the following: ''by the President) that—

''(i) is issued by a court'';

(III) by inserting ''and'' after ''jurisdiction;''; and

(IV) by adding at the end the following:

''(ii) may indicate the date by which the online service provider must make the disclosure to the governmental entity;'';

(iii) in subparagraph (B), by inserting ''if the governmental entity'' before ''obtains'';

(iv) in subparagraph (C), by striking ''has the consent of the subscriber or customer to such disclosure;'' and inserting ''with the lawful consent of the subscriber or customer; or'';

(v) by striking subparagraph (D);

(vi) by redesignating subparagraph (E) as subparagraph (D); and

(vii) in subparagraph (D), as so redesignated, by striking ''seeks information''

and inserting ''as otherwise authorized''; and

(B) in paragraph (2)—

(i) in the matter preceding subparagraph (A), by inserting '', in response to an administrative subpoena authorized by Federal or State statute, a grand jury, trial, or civil discovery subpoena, or any means available under paragraph (1),'' after ''shall''; and

(ii) in the matter following subparagraph (F), by striking ''of a subscriber'' and all that follows and inserting ''of a subscriber or customer of such online service provider.'';

(3) in subsection (d)—

(A) by striking ''the contents of a wire or electronic communication, or'';

(B) by striking ''sought,'' and inserting ''sought''; and

(C) by striking ''section'' and inserting ''subsection''; and

(4) by adding after subsection (j), as added by section 601(c) of this Act, the following:

''(k) NOTICE.—Except as provided in section 2705, an online service provider may notify a subscriber or customer of a receipt of a warrant, court order, subpoena, or request under subsection (a), (c), or (d) of this section.

''(l) RULE OF CONSTRUCTION RELATED TO LEGAL PROCESS.—Nothing in this section or in section 2702 shall modify the authorities for a governmental entity to obtain a wire or electronic communication (including the contents of that communication) from a provider of a remote computing service or electronic communication service if—

''(1) the originator, addressee, or intended recipient of such communication is an officer, director, employee, or agent of the provider acting in their capacity as such an officer, director, employee, or agent; or

''(2) the communication—

''(A) advertises or promotes a product or service; and

''(B) has been made readily available to the general public.

''(m) RULE OF CONSTRUCTION RELATED TO CONGRESSIONAL SUBPOENAS.—Nothing in this section or in section 2702 shall limit the power of inquiry vested in the

Congress by article I of the Constitution of the United States.''.

(d) WARRANT REQUIREMENT FOR STORED COMMUNICATIONS CONTENT.—Section 2703 of title 18, United States Code, is amended—

(1) in subsection (a)—

(A) by striking '', that is in electronic storage in an electronic communications system for one hundred and eighty days or less,''; and

(B) by striking the last sentence;

(2) by striking subsection (b) and inserting the following:

''(b) [Repealed].''; and

(3) in subsection (d) by striking ''(b) or''.

SEC. 604. CONSISTENT PROTECTIONS FOR DEMANDS FOR DATA HELD BY INTERACTIVE COMPUTING SERVICES.

(a) DEFINITION.—Subsection (a) of section 2711 of title 18, United States Code, as so designated and amended by section 601 of this Act, is amended by adding at the end the following:

''(8) the term 'online service provider' means a provider of electronic communication service, a provider of remote computing service, or a provider of an interactive computer service (as defined in section

230(f) of the Communications Act of 1934 (47 U.S.C. 230(f))); and''.

(b) REQUIRED DISCLOSURE.—Section 2703 of title 18, United States Code, is amended—

(1) in subsection (a), in the first sentence, by striking ''a provider of electronic communication service'' and inserting ''an online service provider'';

(2) in subsection (c)—

(A) in paragraph (1), in the matter preceding subparagraph (A), by striking ''a provider of electronic communication service or remote computing service'' and inserting ''an online service provider''; and

(B) in paragraph (2), in the matter preceding subparagraph (A), by striking ''A provider of electronic communication service or remote computing service'' and inserting ''An online service provider''; and

(3) in subsection (g), by striking ''a provider of electronic communications service or remote computing service'' and inserting ''an online service provider''.

SEC. 605. CONSISTENT PROTECTIONS FROM FEDERAL LAW ENFORCEMENT FOR REAL-TIME AND HISTORICAL METADATA.

Chapter 206 of title 18, United States Code, is amended—

(1) in section 3122(b), by striking paragraph (2) and inserting the following:

''(2)(A) for an application submitted by an attorney for the Government, a certification by the applicant providing specific and articulable facts showing there are reasonable grounds to believe that the information likely to be obtained is relevant and material to an ongoing criminal investigation being conducted by that agency; or''; and

(2) in section 3123(a)(1), in the first sentence—

(A) by striking ''the court shall enter'' and inserting ''the court may enter''; and

(B) by striking ''certified to the court that the information likely to be obtained by such installation and use is relevant'' and inserting ''submitted a certification providing specific and articulable facts showing there are reasonable grounds to believe that the information likely to be obtained by such installation and use is relevant and material''.

SEC. 606. SUBPOENAS FOR CERTAIN SUBSCRIBER INFORMATION.

Section 2703(c)(2) of title 18, United States Code, is amended, in the matter following subparagraph (F), as amended by section 603(c) of this Act, by inserting ''with respect to whom the governmental entity identifies the name, address, temporarily assigned network address, or account identifier (such as a user name)'' before the period at the end.

SEC. 607. MINIMIZATION STANDARDS FOR VOLUNTARY DISCLOSURE OF CUSTOMER COMMUNICATIONS OR RECORDS.

(a) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Attorney General shall issue and make publicly available minimization procedures applicable to disclosures to a Federal agency under paragraph (5) or (8) of subsection (b) or paragraph (3) or (4) of subsection (c) of section 2702 of title 18, United States Code.

(b) CONTENTS.—The procedures issued under subsection (a) shall include provisions to—

(1) limit, to the greatest extent possible, the acquisition, use, and dissemination of the contents of communication and records and other information to that which is required for the specific purpose for which the disclosure was intended;

(2) to the greatest extent possible, remove personally identifiable information prior to acquisition;

(3) to the extent personally identifiable information cannot be removed prior to acquisition, mask such information prior to its use or dissemination, consistent with the purpose for which the disclosure was intended; and

(4) ensure that no contents of communications or records or other information are retained by the agency to which the disclosure was made, or any agency to which the contents of communications or records or other information were disclosed, after the completion of the investigation or action for which the disclosure was intended.

SEC. 608. CONSISTENT PRIVACY PROTECTIONS FOR DATA HELD BY DATA BROKERS.

Section 2703 of title 18, United States Code, as amended by section 603 of this Act, is amended by adding at the end the following:

''(n) COVERED PERSONAL DATA.—

''(1) DEFINITIONS.—In this subsection, the terms 'covered personal data' and 'covered organization' have the meanings given such terms in section 2702(e).

"(2) LIMITATION.—Unless a governmental entity obtains an order in accordance with paragraph (3), the governmental entity may not require a covered organization that is not an online service provider to disclose covered personal data if a court order would be required for the governmental entity to require an online service provider to disclose such covered personal data that is a record of a customer or subscriber of the online service provider.

"(3) ORDERS.—

"(A) IN GENERAL.—A court may only issue an order requiring a covered organization that is not an online service provider to disclose covered personal data on the same basis and subject to the same limitations as would apply to a court order to require disclosure by an online service provider.

"(B) STANDARD.—For purposes of subparagraph (A), a court shall apply the most stringent standard under Federal statute or the Constitution of the United States that would be applicable to a request for a court order to require a comparable disclosure by an online service provider of comparable records of a cus-

tomer or subscriber of the online service provider.''.

SEC. 609. PROTECTION OF DATA ENTRUSTED TO INTERMEDIARY OR ANCILLARY SERVICE PROVIDERS.

(a) DEFINITION.—Subsection (a) of section 2711 of title 18, United States Code, as so designated and amended by sections 601 and 604 of this Act, is amended by adding at the end the following:

''(9) the term 'intermediary or ancillary service provider' means an entity or facilities owner or operator that directly or indirectly delivers, transmits, stores, or processes communications or any other covered personal data (as defined in section 2702(e) of this title) for, or on behalf of, an online service provider.''.

(b) PROHIBITION.—Section 2702(a) of title 18, United States Code, is amended—

(1) in paragraph (1), by striking ''and'' at the end;

(2) in paragraph (2)(B), by striking ''and'' at the end;

(3) in paragraph (3), by striking the period at the end and inserting ''; and''; and

(4) by adding at the end the following:

''(4) an intermediary or ancillary service provider may not knowingly disclose—

''(A) to any person or entity the contents of a communication while in electronic storage by that intermediary or ancillary service provider; or

''(B) to any governmental entity a record or other information pertaining to a subscriber to or customer of, a recipient of a communication from a subscriber to or customer of, or the sender of a communication to a subscriber to or customer of, the online service provider for, or on behalf of, which the intermediary or ancillary service provider directly or indirectly delivers, transmits, stores, or processes communications or any other covered personal data (as defined in subsection (e)).''.

SEC. 610. MODERNIZING CRIMINAL SURVEILLANCE REPORTS.

(a) REPORTS CONCERNING ACCESS TO CUSTOMER COMMUNICATIONS OR RECORDS.—

(1) IN GENERAL.—Section 2703 of title 18, United States Code, as amended by section 608 of this Act, is amended by adding at the end the following:

''(o) REPORTS CONCERNING ACCESS TO CUSTOMER COMMUNICATIONS OR RECORDS.—

''(1) IN GENERAL.—In January of each year, any judge who has issued an order under this section or a warrant to obtain records described in this section, or who has denied approval of an application under this section during the preceding year, shall report to the Administrative Office of the United States Courts—

''(A) the fact that the order or warrant was applied for;

''(B) the type of records sought in the order or warrant;

''(C) whether the order or warrant was—

''(i) granted as applied for;

''(ii) granted as modified; or

''(iii) denied;

''(D) the subsection of this section under which the application for the order or warrant was filed;

''(E) the nature of the offense or criminal investigation that was the basis for the application for the order or warrant;

''(F) the name of each provider of electronic communication service or remote com-

puting service served with the order or warrant, if so granted; and

"(G) the investigative or law enforcement agency that submitted the application.

"(2) PUBLIC REPORT.—In June of each year, the Director of the Administrative Office of the United States Courts shall publish on the website of the Administrative Office of the United States Courts and include in the report required under section 2519(3)—

"(A) a full and complete report concerning the number of applications for orders or warrants requiring the disclosure of, during the preceding calendar year—

"(i) the contents of wire or electronic communications in electronic storage under subsection (a); and

"(ii) records concerning electronic communication service or remote computer service under subsection (c);

"(B) the number of orders and warrants granted or denied under this section during the preceding calendar year; and

"(C) a detailed summary and analysis of each category of data required to be filed with

the Administrative Office of the United States Courts under paragraph (1).

''(3) FORMAT.—Not later than 180 days after the date of enactment of the Government Surveillance Reform Act of 2026, the Director of the Administrative Office of the United States Courts shall, in consultation with the National Institute of Standards and Technology, the Administrator of General Services, the Electronic Public Access Public User Group, private entities offering electronic case management software, the National Center for State Courts, and the National American Indian Court Judges Association, publish a machine readable form that shall be used for any report required under paragraph (1).

''(4) REGULATIONS.—The Director of the Administrative Office of the United States Courts may issue binding regulations with respect to the content and form of the reports required under paragraph (1).''.

(2) TECHNICAL AND CONFORMING AMENDMENT.—Section 2519(3) of title 18, United States Code, is amended, in the first sentence, by inserting ''publish on the website of the Administrative Office of the United States Courts and'' before ''transmit''.

(b) REPORTS CONCERNING PEN REGISTERS AND TRAP AND TRACE DEVICES.—Section 3126 of title 18, United States Code, is amended to read as follows:

"§ 3126. Reports concerning pen registers and trap and trace devices

''(a) IN GENERAL.—In January of each year, any judge who has issued an order (or an extension thereof) under section 3123 that expired during the preceding year, or who has denied approval of an installation and use of a pen register or trap and trace device during that year, shall report to the Administrative Office of the United States Courts—

''(1) the fact that an order or extension was applied for;

''(2) the kind of order or extension applied for;

''(3) the fact that the order or extension was granted as applied for, was modified, or was denied;

''(4) the period of installation and use of a pen register or trap and trace device authorized by the order, and the number and duration of any extensions of the order;

''(5) the offense specified in the order or application, or extension of an order;

''(6) the precise nature of the facilities affected and the precise nature of the information sought; and

''(7) the investigative or law enforcement agency that submitted the application.

''(b) PUBLIC REPORT.—In June of each year, the Director of the Administrative Office of the United States Courts shall publish on the website of the Administrative Office of the United States Courts and include in the report required under section 2519(3)—

''(1) a full and complete report concerning—

''(A) the number of applications for orders authorizing or approving the installation and use of a pen register or trap and trace device pursuant to this chapter; and

''(B) the number of orders and extensions granted or denied pursuant to this chapter during the preceding calendar year; and

''(2) a detailed summary and analysis of each category of data required to be reported under subsection (a).

''(c) FORMAT.—Not later than 180 days after the date of enactment of the Government Surveillance Reform Act of 2026, the Director of the Administrative Office of the United States Courts shall, in consultation with the

National Institute of Standards and Technology and the Administrator of General Services, private entities offering electronic case management software, the National Center for State Courts, and the National American Indian Court Judges Association, publish a machine readable form that shall be used for any report required under subsection (a).

''(d) REGULATIONS.—The Director of the Administrative Office of the United States Courts may issue binding regulations with respect to the content and form of the reports required under subsection (a).''.

(c) REPORTING OF VOLUNTARY DISCLOSURES.—Section 2702(d) of title 18, United States Code, is amended—

(1) in the heading, by striking ''EMERGENCY'' and inserting ''VOLUNTARY'';

(2) in the matter preceding paragraph (1), by inserting ''and publish on the website of the Department of Justice'' after ''Senate'';

(3) in paragraph (1)—

(A) by striking ''the Department of Justice'' and inserting ''each Federal agency''; and

(B) by striking ''subsection (b)(8)'' and inserting ''paragraph (5) or (8) of subsection (b) or paragraph (3) or (4) of subsection (c), broken down by each such paragraph'';

(4) in paragraph (2)(A)—

(A) by striking ''Department of Justice'' and inserting ''Federal agency''; and

(B) by striking ''subsection (b)(8)'' and inserting ''paragraph (5) or (8) of subsection (b) or paragraph (3) or (4) of subsection (c)''; and

(5) by striking paragraph (3).

SEC. 611. LIMITATION OF AMENDMENTS TO FEDERAL DEPARTMENTS AND AGENCIES.

(a) IN GENERAL.—

(1) VOLUNTARY DISCLOSURE.—

(A) IN GENERAL.—Section 2702 of title 18, United States Code, is amended by adding after subsection (g), as added by section 201 of this Act, the following:

''(h) SPECIAL PROCEDURES FOR VOLUNTARY DISCLOSURE TO NON-FEDERAL ENTITIES.—

''(1) IN GENERAL.—The prohibitions in subsection (a) shall not apply to disclosures to a State or local governmental entity.

''(2) SPECIFIC PROHIBITIONS.—Except as provided in paragraphs (3) and (4)—

''(A) a person or entity providing an electronic communication service to the public shall not knowingly divulge to a department or agency of a State or local government the contents

of a communication while in electronic storage by that service;

''(B) a person or entity providing remote computing service to the public shall not knowingly divulge to a department or agency of a State or local government the contents of any communication which is carried or maintained on that service—

''(i) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service; and

''(ii) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and

''(C) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to

or customer of such service (not including the contents of communications covered by subparagraph (A) or (B)) to a department or agency of a State or local government.

''(3) EXCEPTIONS FOR DISCLOSURE OF COMMUNICATIONS.—A provider described in paragraph (2) may divulge the contents of a communication—

''(A) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

''(B) as otherwise authorized in section 2517, 2511(2)(a), or 2703A of this title;

''(C) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

''(D) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

''(E) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

''(F) to a law enforcement agency of a State or local government, if the contents—

''(i) were inadvertently obtained by the service provider; and

''(ii) appear to pertain to the commission of a crime; or

''(G) to a department or agency of a State or local government, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.

''(4) EXCEPTIONS FOR DISCLOSURE OF CUSTOMER RECORDS.—A provider described in paragraph (2) may divulge a record or other information pertaining to a subscriber to or a customer of such service (not including the contents of communications covered by subparagraph (A) or (B) of paragraph (2))—

''(A) as otherwise authorized in section 2703A;

''(B) with the lawful consent of the customer or subscriber;

''(C) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; or

''(D) to a department or agency of a State or local government, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency.''.

(2) REQUIRED DISCLOSURE.—

(A) IN GENERAL.—Section 2703 of title 18, United States Code is amended—

(i) in the section heading, by adding ''**to Federal departments and agencies**'' at the end; and

(ii) by adding after subsection (o), as added by section 610 of this Act, the following:

''(p) LIMITATION TO FEDERAL ENTITIES.—Notwithstanding section 2711, in this section, the term 'governmental entity'—

''(1) means a department or agency of the United States; and

''(2) does not include a department or agency of a State or a political subdivision thereof.''.

(B) PROCEDURES FOR NON-FEDERAL ENTITIES.—Chapter 121 of title 18, United States

Code, is amended by inserting after section 2703 the following:

"§ 2703A. Required disclosure of customer communications or records to State and local departments and agencies

''(a) CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS IN ELECTRONIC STORAGE.—A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures and, in the case of a court-martial or other proceeding under chapter 47 of title 10 (the Uniform Code of Military Justice), issued under section 846 of that title, in accordance with regulations prescribed by the President) by a court of competent jurisdiction. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days

by the means available under subsection (b) of this section.

''(b) CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS IN A REMOTE COMPUTING SERVICE.—(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

''(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures and, in the case of a court-martial or other proceeding under chapter 47 of title 10 (the Uniform Code of Military Justice), issued under section 846 of that title, in accordance with regulations prescribed by the President) by a court of competent jurisdiction; or

''(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

''(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

''(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

''(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service—

''(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

''(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

''(c) RECORDS CONCERNING ELECTRONIC COMMUNICATION SERVICE OR REMOTE COMPUTING SERVICE.—(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including

the contents of communications) only when the governmental entity—

''(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures and, in the case of a court-martial or other proceeding under chapter 47 of title 10 (the Uniform Code of Military Justice), issued under section 846 of that title, in accordance with regulations prescribed by the President) by a court of competent jurisdiction;

''(B) obtains a court order for such disclosure under subsection (d) of this section;

''(C) has the consent of the subscriber or customer to such disclosure;

''(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or

''(E) seeks information under paragraph (2).

''(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the—

''(A) name;

''(B) address;

''(C) local and long distance telephone connection records, or records of session times and durations;

''(D) length of service (including start date) and types of service utilized;

''(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

''(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

''(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

''(d) REQUIREMENTS FOR COURT ORDER.—A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. Such a court order shall not issue if prohibited by the law of the applicable State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

''(e) NO CAUSE OF ACTION AGAINST A PROVIDER DISCLOSING INFORMATION UNDER THIS CHAPTER.—No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.

''(f) REQUIREMENT TO PRESERVE EVIDENCE.—

''(1) IN GENERAL.—A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

''(2) PERIOD OF RETENTION.—Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

''(g) PRESENCE OF OFFICER NOT REQUIRED.—Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

''(h) LIMITATION TO NON-FEDERAL ENTITIES.—Notwithstanding section 2711, in this section, the term 'governmental entity'—

''(1) means a department or agency of a State or a political subdivision thereof; and

''(2) does not include a department or agency of the United States.''.

(3) TRACKING ORDERS BY DEPARTMENTS AND AGENCIES OF STATES AND LOCAL GOVERNMENTS.—Chapter 205 of title 18, United States Code, is amended by inserting after section 3117 the following:

''§ 3117A. Mobile tracking devices for State and local departments and agencies

''(a) IN GENERAL.—If a court is empowered to issue a warrant or other order for the installation of a mobile tracking device, such order may authorize the use of that device by a department or agency of a State or a political subdivision of a State within the jurisdiction of the court, and outside that jurisdiction if the device is installed in that jurisdiction.

''(b) DEFINITION.—As used in this section, the term 'tracking device' means an electronic or mechanical device which permits the tracking of the movement of a person or object.''.

(4) CONSISTENT PROTECTIONS FROM STATE AND LOCAL LAW ENFORCEMENT FOR REAL-TIME AND HISTORICAL METADATA.—Section 3122(b)(2) of title 18, United States Code, as amended by section

605(1) of this Act, is amended by inserting after subparagraph (A) the following:

''(B) for an application submitted by a State law enforcement or investigative officer, a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.''.

(b) LIMITATION ON FEDERAL GOVERNMENTAL ENTITIES .—

(1) IN GENERAL.—A department or agency of the United States may not obtain or acquire any communications, data, records, or other information, or any evidence derived therefrom, from a department or agency of a State or a political subdivision thereof that was obtained or acquired by the department or agency of a State or political subdivision thereof in a manner that would be a violation of Federal law if obtained or acquired by the department or agency of the United States, or in a manner that would not satisfy the legal standards applicable to the department or agency of the United States.

(2) LIMITATION OF USE AS EVIDENCE.—Communications, data, records, other information, or evidence obtained or acquired in violation of paragraph (1), and any evidence derived therefrom, may not be

used, received in evidence, or otherwise disseminated by, on behalf of, or upon a motion or other action by a department or agency of the United States in any investigation, trial, hearing, or other proceeding by, in, or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof.

(3) USE BY AGGRIEVED PARTIES.—Nothing in paragraph (2) shall be construed to limit the use of any information by a person aggrieved of a violation of paragraph (1) in connection with any action relating to such a violation.

(c) TECHNICAL AND CONFORMING AMENDMENTS.—

(1) HOMELAND SECURITY ACT OF 2002.—The Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is amended—

(A) in section 2207(d)(2) (6 U.S.C. 657(d)(2)), by striking ''section 2702(b)'' and inserting ''subsection (b) or (h) of section 2702, as applicable,''; and

(B) in section 2220C(e) (6 U.S.C. 665i(e)), by striking ''section 2702'' and inserting ''subsection (b) or (h) of section 2702, as applicable,''.

(2) CHAPTER 110.—Chapter 110 of title 18, United States Code, is amended—

(A) in section 2258A(g)(4), by inserting ''or subparagraphs (C) through (G) of section 2702(h)(3), as applicable'' after ''section 2702(b)''; and

(B) in section 2258B—

(i) in subsection (b)(2)(C), by striking ''sections 2258A, 2258C, 2702, or 2703'' and inserting ''section 2258A, section 2258C, subsection (b) or (h) of section 2702 (as applicable), or section 2703 or 2703A (as applicable)''; and

(ii) in subsection (d)(2)(B)(iii)(II), by striking ''sections 2258A, 2258C, 2702, or 2703'' and inserting ''section 2258A, section 2258C, subsection (b) or (h) of section 2702 (as applicable), or section 2703 or 2703A (as applicable)''.

(3) CHAPTER 121.—Chapter 121 of title 18, United States Code, is amended—

(A) in section 2701(c)(3), by striking ''section 2703'' and inserting ''section 2703 or 2703A (as applicable)'';

(B) in section 2705—

(i) by striking ''section 2703(b)'' each place it appears and inserting ''section 2703A(b)'';

(ii) in subsection (a)(4), by striking ''section 2703'' and inserting ''section 2703 or 2703A, as applicable,''; and

(iii) in subsection (b), in the matter preceding paragraph (1)—

(I) by striking ''section 2703'' and inserting ''section 2703 or 2703A, as applicable,''; and

(II) by striking ''section 2703(b)(1)'' and inserting ''section 2703A(b)(1)'';

(C) in section 2706—

(i) in subsection (a), by striking ''section 2702, 2703, or 2704 of this title'' and inserting ''subsection (b) or (h) of section 2702 (as applicable), section 2703 or 2703A (as applicable), or section 2704''; and

(ii) in subsection (c), by striking ''section 2703 of this title'' and inserting ''section 2703 or 2703A, as applicable''; and

(D) in section 2707—

(i) in subsection (a), by striking ''section 2703(e),'' and inserting ''section 2703(e) or section 2703A(e), as applicable,'';

(ii) in subsection (e)(1), by striking ''section 2703(f) of this title'' and inserting ''section 2703(f) or section 2703A(f), as applicable''; and

(iii) in subsection (g), by striking ''section 2703 of this title,'' and inserting ''section 2703 or 2703A, as applicable,''.

(4) DEFINITION OF ELECTRONIC COMMUNICATION.—Section 2510(12)(C) of title 18, United States Code, is amended to read as follows:

''(C)(i) in the case of a department or agency of the United States, a communication from a lawfully installed tracking device (as defined in section 3117 of this title), if—

''(I) the tracking device is physically placed; or

''(II) the tracking software or functionality of the tracking device is remotely activated and the communication is transmitted by the tracking software or

functionality as a result of the remote activation; or

''(ii) in the case of a department or agency of a State or a political subdivision thereof, any communication from a tracking device (as defined in section 3117A of this title); or''.

(5) CHAPTER 121 TABLE OF SECTIONS.—The table of sections for chapter 121 of title 18, United States Code, is amended by striking the item relating to section 2703 and inserting the following:

''2703. Required disclosure of customer communications or records to Federal departments and agencies.
''2703A. Required disclosure of customer communications or records to State and local departments and agencies.''.

(6) CHAPTER 205 TABLE OF SECTIONS.—The table of sections for chapter 205 of title 18, United States Code, is amended by striking the item relating to section 3117 and inserting the following:

''3117. Tracking orders for Federal departments and agencies.
''3117A. Mobile tracking devices for State and local departments and agencies.''.

(d) CONFORMING AMENDMENTS TO THE EMAIL PRIVACY ACT.—Section 2704 of title 18, United States Code, is amended—

(1) in subsection (a)—

(A) in paragraph (1), by striking ''section 2703(b)(2)'' and inserting ''section 2703A(b)(2)''; and

(B) in paragraph (5), by striking ''section 2703'' and inserting ''section 2703A''; and

(2) by adding at the end the following:

''(c) LIMITATION TO NON-FEDERAL ENTITIES.—Notwithstanding section 2711, in this section, the term 'governmental entity'—

''(1) means a department or agency of a State or a political subdivision thereof; and

''(2) does not include a department or agency of the United States.''.

TITLE VII—PROTECTION OF CAR DATA FROM FEDERAL WARRANTLESS SEARCHES

SEC. 701. PROTECTION OF CAR DATA FROM FEDERAL WARRANTLESS SEARCHES.

(a) IN GENERAL.—Part I of title 18, United States Code, is amended by adding at the end the following:

''CHAPTER 124—ACCESSING VEHICLE DATA

''§ 2730. Definitions

''In this chapter:

''(1) ACCESS.—The term 'access' means any retrieval of covered vehicle data, regardless of—

"(A) whether the data is obtained as the information is being produced or from digital storage; and

"(B) where the vehicle data is stored or transmitted, including by wire or radio.

"(2) CONSENT.—The term 'consent'—

"(A) means an affirmative, express, and voluntary agreement that—

"(i) states that the person providing the consent is providing consent to a government official to access the digital contents, access credential, or online account information, or other information being sought;

"(ii) specifies the type of content, access credential, or online account information the person is providing access to;

"(iii) specifies the time period of the covered vehicle data to be accessed;

"(iv) informs the person providing consent that consent is optional and that the government official attempting to obtain consent must otherwise acquire a warrant if consent is not obtained;

''(v) does not involve sanctions or the threat of sanctions for withholding consent; and

''(vi) uses clear, simple, and comprehensible language that is presented in a way that is accessible to the person providing consent; and

''(B) does not include consent obtained through agreement to a generic privacy policy or a terms of service agreement.

''(3) COVERED VEHICLE DATA.—The term 'covered vehicle data'—

''(A) means all onboard and telematics data generated by, processed by, or stored on a noncommercial vehicle using computing, storage and communication systems installed, attached to, or carried in the vehicle, including diagnostic data, entertainment system data, navigation data, images or data captured by onboard sensors, or cameras, including images or data used to support automated features or autonomous driving, internet access, and communication to and from vehicle occupants;

''(B) includes data gathered by event data recorders; and

"(C) does not include—

"(i) automotive software installed by the manufacturer, as defined by applicable industry standards or regulations;

"(ii) any data subject to chapter 119 of this title or section 104 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1804); or

"(iii) data that is collected from outside the vehicle, including speed data and geolocation data, for purposes of traffic, law enforcement, or toll collection.

"(4) EVENT DATA RECORDER.—The term 'event data recorder' has the meaning given the term in section 563.5 of title 49, Code of Federal Regulations (as in effect on March 5, 2019).

"(5) FEDERAL INVESTIGATIVE OR LAW ENFORCEMENT OFFICER.—The term 'Federal investigative or law enforcement officer' means any officer of the United States, who is empowered by law to execute searches, to seize evidence, or to make arrests for a violation of any Federal law.

"(6) NONCOMMERCIAL VEHICLE.—The term 'noncommercial vehicle' has the meaning given the

term 'non-CMV' in section 383.5 of title 49, Code of Federal Regulations.

''(7) VEHICLE OPERATOR.—The term 'vehicle operator' means—

''(A) a person who controls the operation of a vehicle at the time consent is sought; and

''(B) with respect to a vehicle that is not classified as a highly autonomous vehicle by the Secretary of Transportation, the driver of the vehicle.

''§ 2731. Prohibition on Federal access to vehicle data

''(a) IN GENERAL.—Except as provided in subsection (b), a Federal investigative or law enforcement officer may not access covered vehicle data unless pursuant to a warrant issued in accordance with the procedures described in rule 41 of the Federal Rules of Criminal Procedure by a court of competent jurisdiction, or as otherwise provided in this chapter or sections 104 and 303 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1804, 1823).

''(b) EXCEPTIONS.—

''(1) CONSENT.—

''(A) IN GENERAL.—A Federal investigative or law enforcement officer may access covered vehicle data if—

"(i) the vehicle operator provides prior consent to such access; and

"(ii) no passenger 14 years of age or older objects to the access.

"(B) VEHICLE OWNER.—If the vehicle operator cannot be located with reasonable effort, the vehicle owner or, in the case of a leased vehicle, the lessee, may provide consent under this paragraph.

"(C) UNLAWFUL POSSESSION.—No individual may provide or withhold consent under this paragraph or object to another individual accessing covered vehicle data if the individual—

"(i) is the vehicle operator who is in unlawful possession of the vehicle; or

"(ii) is a passenger who unlawfully obtained access to the vehicle.

"(D) ORAL CONSENT.—Consent provided under this paragraph shall be in writing unless—

"(i) the person providing the consent requests that the consent be made orally; and

''(ii) the request for consent and the consent are recorded.

''(E) CONSENT OF VEHICLE OPERATOR.—If the vehicle operator is not the owner of the vehicle and provides consent under this paragraph, the consent is valid only with respect to covered vehicle data generated during the lawful possession and use of the vehicle by the vehicle operator.

''(2) EMERGENCY.—

''(A) IN GENERAL.—A Federal investigative or law enforcement officer, the Attorney General, the Deputy Attorney General, or the Associate Attorney General may access covered vehicle data if—

''(i) such officer reasonably determines that an emergency situation exists that—

''(I) involves immediate danger of death or serious physical injury to any person; and

''(II) requires access to covered vehicle data before such officer can, with due diligence, obtain a warrant;

"(ii) there are grounds upon which a warrant could be granted to authorize such access; and

"(iii) an application for a warrant approving such access is submitted to a court within 48 hours after the access has occurred or begins to occur.

"(B) DENIAL.—If an application for a warrant submitted pursuant to subparagraph (A)(iii) is denied, any covered vehicle data accessed under this paragraph shall be treated as having been obtained in violation of this chapter.

"(3) EVENT DATA RECORDER FOR MOTOR VEHICLE SAFETY.—In addition to the exceptions in paragraphs (1) and (2), data recorded or transmitted by an event data recorder may be accessed from a noncommercial vehicle if authorized by paragraph (3), (4), or (5) of section 24302(b) of the Driver Privacy Act of 2015 (49 U.S.C. 30101 note).

"(4) RULE OF CONSTRUCTION.—Nothing in this section shall be interpreted to require the transmission or storage of data that is not otherwise transmitted or stored, or the retrieval of data that is not generally retrievable.

"§ 2732. Prohibition on use of acquired information as evidence

''(a) IN GENERAL.—If any covered vehicle data has been acquired in violation of this chapter, no part of such information and no evidence derived therefrom may be used, received in evidence, or otherwise disseminated in any investigation, trial, hearing, or other proceeding by, in, or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof.

''(b) PROBABLE CAUSE.—No data described in section 2731(b)(3) may be used to establish probable cause.''.

(b) TECHNICAL AND CONFORMING AMENDMENTS.—

(1) DRIVER PRIVACY ACT OF 2015.—Section 24302 of the Driver Privacy Act of 2015 (49 U.S.C. 30101 note) is amended—

(A) in subsection (b), in the matter preceding paragraph (1), by striking ''Data'' and inserting ''Except as provided in subsection (c), data''; and

(B) by adding at the end the following:

''(c) FEDERAL INVESTIGATIVE OR LAW ENFORCEMENT OFFICERS.—A Federal investigative or law enforcement officer (as defined in section 2730 of title 18, United States Code), may only access or retrieve data recorded

or transmitted by an event data recorder described in subsection (a) in accordance with chapter 124 of title 18, United States Code.''.

(2) TABLE OF CHAPTERS.—The table of chapters for part 1 of title 18, United States Code, is amended by adding at the end the following:

''124. Accessing vehicle data ..... 2730''.

TITLE VIII—INTELLIGENCE TRANSPARENCY

SEC. 801. 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).''.

SEC. 802. ENHANCED ANNUAL REPORTS BY DIRECTOR OF NATIONAL INTELLIGENCE.

(a) IN GENERAL.—Subsection (b) of section 603 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1873(b)) is amended—

(1) in paragraph (2)(C), by striking the semicolon and inserting ''; and'';

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

(3) 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

(4) 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 302 of the Government Surveillance Reform Act of 2026; 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 302 of the Government Surveillance Reform Act of 2026; 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.''.

(b) REPEAL OF NONAPPLICABILITY TO FEDERAL BUREAU OF INVESTIGATION OF CERTAIN REQUIREMENTS.—Subsection (d) of such section is amended—

(1) by striking paragraph (2); and

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

(c) CONFORMING AMENDMENT.—Subsection (d)(1) of such section is amended by striking ''paragraphs (3), (5), or (6)'' and inserting ''paragraph (6), (8), or (9)''.

SEC. 803. 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 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 to improve compliance and accuracy.

''(2) INSPECTOR GENERAL RISK ASSESSMENT.—In addition to conducting audits under section 501 of the Government Surveillance Reform Act of 2026, 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.''.

SEC. 804. ALLOWING MORE GRANULAR AGGREGATE REPORTING BY RECIPIENTS OF FOREIGN INTELLIGENCE SURVEILLANCE ORDERS.

(a) MODIFICATION OF AGGREGATION BANDING.—Subsection (a) of section 604 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1874) is amended—

(1) 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 first 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 first 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 first 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 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 first 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 first 1000 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 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 first 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

(2) by redesignating paragraph (4) as paragraph (2).

(b) ADDITIONAL DISCLOSURES.—Such section is amended—

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

(2) 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(f)(3).''.

(c) CONFORMING AMENDMENTS.—Subsection (c) of such section, as redesignated by subsection (b)(1) of this section, is amended—

(1) in paragraph (1), by striking ''or (2)'';

(2) by striking paragraph (2);

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

(4) in paragraph (2), as so redesignated, by striking ''(4)'' and inserting ''(2)''.

SEC. 805. REPORT ON USE OF FOREIGN INTELLIGENCE SURVEILLANCE AUTHORITIES REGARDING PROTECTED ACTIVITIES AND PROTECTED CLASSES.

(a) REPORT.—Not later than 1 year after the date of the enactment of this Act, 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 activities and protected classes described in subsection (b) in—

(1) 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

(2) investigations for which such orders are sought.

(b) ACTIVITIES AND PROTECTED CLASSES DESCRIBED.—The activities and protected classes described in this subsection are the following:

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

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

(c) FORM.—In addition to the report made publicly available and submitted under subsection (a), the Board

may submit to the appropriate committees of Congress a classified annex.

SEC. 806. PUBLICATION OF ESTIMATES REGARDING COMMUNICATIONS COLLECTED UNDER CERTAIN PROVISIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

Not later than 90 days after the date of the 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.

SEC. 807. ENHANCED REPORTING OF ASSESSMENTS OF COMPLIANCE WITH EMERGENCY ORDER REQUIREMENTS UNDER CERTAIN PROVISIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

(a) ELECTRONIC SURVEILLANCE.—

(1) 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''.

(2) REPORTING.—Section 108(a)(2) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1808(a)(2)) is amended—

(A) in subparagraph (C), by striking ''; and'' and inserting a semicolon;

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

(C) by adding at the end the following:

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

(b) PHYSICAL SEARCHES.—

(1) 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''.

(2) REPORTING.—Section 306 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1826) is amended—

(A) in paragraph (3), by striking ''; and'' and inserting a semicolon;

(B) in paragraph (4), by striking the period and inserting ''; and''; and

(C) by adding at the end the following:

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

TITLE IX—SEVERABILITY AND LIMITED DELAYS IN IMPLEMENTATION

SEC. 901. RULE OF CONSTRUCTION WITH RESPECT TO STATE AND LOCAL LAW ENFORCEMENT AUTHORITIES.

Nothing in this Act, or an amendment made by this Act, shall be construed to modify the authorities or affect the procedures for the acquisition of records by any department or agency of a State or a political subdivision thereof as in effect on the day before the date of the enactment of this Act.

SEC. 902. SEVERABILITY.

If any provision of this Act, an amendment made by this Act, or the application of such a provision or amendment to any person or circumstance, is held to be unconstitutional, the remaining provisions of and amendments made by this Act, and the application of the provision or amendment held to be unconstitutional to any other person or circumstance, shall not be affected thereby.

SEC. 903. LIMITED DELAYS IN IMPLEMENTATION.

The Attorney General may, in coordination with the Director of National Intelligence as may be appropriate, delay implementation of a provision of this Act or an amendment made by this Act for a period of not more than 1 year upon a showing to the appropriate committees of Congress that the delay is necessary—

(1) to develop and implement technical systems needed to comply with the provision or amendment; or

(2) to hire or train personnel needed to comply with the provision or amendment.

○