

Calendar No. 371

119TH CONGRESS
2D SESSION**S. 4280**

To amend the Foreign Intelligence Surveillance Act of 1978 to reauthorize and reform certain authorities and to provide greater transparency and oversight.

IN THE SENATE OF THE UNITED STATES

APRIL 13, 2026

Mr. LEE (for himself and Mr. DURBIN) introduced the following bill; which was read the first time

APRIL 14, 2026

Read the second time and placed on the calendar

A BILL

To amend the Foreign Intelligence Surveillance Act of 1978 to reauthorize and reform certain authorities and to provide greater transparency and oversight.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**

4 (a) SHORT TITLE.—This Act may be cited as the
5 “Security And Freedom Enhancement Act of 2026” or the
6 “SAFE Act”.

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

Sec. 1. Short title; table of contents.

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

Sec. 101. Query procedure reform.

Sec. 102. Annual reports.

Sec. 103. Accountability and reporting procedures for compliance violations relating to queries conducted by the Federal Bureau of Investigation.

Sec. 104. Prohibition on reverse targeting of United States persons and persons located in the United States.

Sec. 105. FISA court review of targeting decisions.

Sec. 106. Sunset of changes to definition of electronic communication service provider.

Sec. 107. Limitation on directives under Foreign Intelligence Surveillance Act of 1978 relating to certain electronic communication service providers.

Sec. 108. Extension of title VII of FISA; expiration of FISA authorities; effective dates.

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

Sec. 201. Required disclosure of information and limits on use of certain information and on issuance of orders.

Sec. 202. Criminal penalties for violations of FISA.

Sec. 203. Agency procedures To ensure compliance.

Sec. 204. Limit on civil immunity for providing information, facilities, or technical assistance to the Government absent a court order.

Sec. 205. Prohibition on avoiding disclosure obligations through parallel construction.

Sec. 206. Sunset on grandfather clause of FISA's business records provision.

TITLE III—REFORMS RELATING TO PROCEEDINGS BEFORE THE
 FOREIGN INTELLIGENCE SURVEILLANCE COURT AND OTHER
 COURTS

Sec. 301. Foreign Intelligence Surveillance Court reform.

Sec. 302. Public disclosure and declassification of certain documents.

Sec. 303. Technical amendment to contempt power of FISC and FISC-R.

TITLE IV—INDEPENDENT EXECUTIVE BRANCH OVERSIGHT

Sec. 401. Periodic audit of FISA compliance by Inspector General.

TITLE V—PROTECTIONS FOR UNITED STATES PERSONS WHOSE
 SENSITIVE INFORMATION IS PURCHASED BY INTELLIGENCE
 AND LAW ENFORCEMENT AGENCIES

Sec. 501. Limitation on intelligence acquisition of United States person data.

Sec. 502. Limitation on law enforcement purchase of personal data from data brokers.

Sec. 503. Consistent protections for demands for data held by interactive computing services.

Sec. 504. Consistent privacy protections for data held by data brokers.

Sec. 505. Protection of data entrusted to intermediary or ancillary service providers.

TITLE VI—TRANSPARENCY

Sec. 601. Enhanced reports by Director of National Intelligence.

Sec. 602. Notification to Congress of certain unauthorized disclosures.

TITLE VII—LIMITED DELAYS IN IMPLEMENTATION

Sec. 701. Limited delays in implementation.

1 **TITLE I—PROTECTIONS FOR** 2 **UNITED STATES PERSONS** 3 **WHOSE COMMUNICATIONS** 4 **ARE COLLECTED UNDER SEC-** 5 **TION 702 OF THE FOREIGN IN-** 6 **TELLIGENCE SURVEILLANCE** 7 **ACT OF 1978**

8 **SEC. 101. QUERY PROCEDURE REFORM.**

9 (a) MANDATORY AUDITS OF UNITED STATES PER-
10 SON QUERIES CONDUCTED BY FEDERAL BUREAU OF IN-
11 VESTIGATION.—

12 (1) IN GENERAL.—The Department of Justice
13 shall conduct an audit that reviews each covered
14 query, as defined in paragraph (8) of section 702(f)
15 of the Foreign Intelligence Surveillance Act of 1978
16 (50 U.S.C. 1881a(f)), as redesignated and amended
17 by subsection (b) of this section, conducted during
18 the 180-day period beginning on the date of enact-

1 ment of this Act, and during each 180-day period
2 thereafter.

3 (2) COMPLETION OF AUDIT.—

4 (A) IN GENERAL.—Not later than 90 days
5 after the end of each 180-day period described
6 in paragraph (1), the Department of Justice
7 shall complete the audit described in such para-
8 graph with respect to such 180-day period.

9 (B) SUBMISSION TO CONGRESS.—Not later
10 than 30 days after completing each audit re-
11 quired under paragraph (1), the Department of
12 Justice shall submit to the appropriate commit-
13 tees of Congress the complete and unredacted
14 results of the audit.

15 (C) BRIEFING REGARDING UNTIMELY AU-
16 DITS.—If the Department of Justice fails to
17 complete and send the results of an audit re-
18 quired under paragraph (1) to the appropriate
19 committees of Congress on or before the date
20 that 120 days after the end of the 180-day pe-
21 riod to which the audit relates, not later than
22 127 days after the end of such 180-day period,
23 the Department of Justice shall conduct an in-
24 person briefing with the appropriate committees
25 of Congress.

1 (D) DEFINITION.—In this paragraph, the
 2 term “appropriate committees of Congress”
 3 means—

4 (i) the congressional intelligence com-
 5 mittees (as defined in section 3 of the Na-
 6 tional Security Act of 1947 (50 U.S.C.
 7 3003));

8 (ii) the Committee on the Judiciary of
 9 the Senate; and

10 (iii) the Committee on the Judiciary
 11 of the House of Representatives.

12 (3) REPEAL OF SUPERSEDED AUDIT REQUIRE-
 13 MENT.—Section 2(c) of the Reforming Intelligence
 14 and Securing America Act (50 U.S.C. 1881a note)
 15 is repealed.

16 (b) RESTRICTIONS RELATING TO CONDUCT OF CER-
 17 TAIN QUERIES BY FEDERAL BUREAU OF INVESTIGA-
 18 TION.—Section 702(f) of the Foreign Intelligence Surveil-
 19 lance Act of 1978 (50 U.S.C. 1881a(f)) is amended—

20 (1) by redesignating paragraph (5) as para-
 21 graph (8);

22 (2) by inserting before paragraph (8), as so re-
 23 designated, the following:

24 “(7) QUERYING PROCEDURES APPLICABLE TO
 25 FEDERAL BUREAU OF INVESTIGATION.—For any

1 procedures adopted under paragraph (1) applicable
2 to the Federal Bureau of Investigation, the Attorney
3 General, in consultation with the Director of Na-
4 tional Intelligence, shall include the following re-
5 quirements:

6 “(A) TRAINING.—A requirement that,
7 prior to conducting any query, and on an an-
8 nual basis thereafter as a prerequisite for con-
9 tinuing to conduct queries, personnel of the
10 Federal Bureau of Investigation successfully
11 complete training on the querying procedures.

12 “(B) ADDITIONAL PRIOR APPROVALS FOR
13 SENSITIVE QUERIES.—A requirement that, ab-
14 sent exigent circumstances, prior to conducting
15 certain queries, personnel of the Federal Bu-
16 reau of Investigation receive approval, at min-
17 imum, as follows:

18 “(i) Approval from an attorney at the
19 Federal Bureau of Investigation if the
20 query uses a query term reasonably be-
21 lieved to identify a United States elected
22 official, a governor of a State, an appointee
23 of the President or the governor of a State,
24 a United States political candidate, a
25 United States political organization or a

United States person prominent in such organization, a United States media organization or a United States person who is a member of such organization, a justice, judge, bankruptcy judge, or magistrate judge of the United States, or a judge or justice of the highest court of a State.

“(ii) Approval from an attorney of the Federal Bureau of Investigation if the query uses a query term reasonably believed to identify a United States religious organization or a United States person who is prominent in such organization.

“(iii) Approval from an attorney of the Federal Bureau of Investigation for 2 or more queries conducted together, including through the use of batch job technology, any successor tool, or any other batch query method.

“(C) PRIOR WRITTEN JUSTIFICATION.—A requirement that—

“(i) prior to conducting a covered query, personnel of the Federal Bureau of Investigation generate a written statement of the specific factual basis to support the

1 reasonable belief that such query meets the
2 standards required by the procedures
3 adopted under paragraph (1), which shall,
4 for each covered query relating to the same
5 United States person or persons, explain
6 and support each individual query; and

7 “(ii) for each covered query, the Fed-
8 eral Bureau of Investigation shall keep a
9 record of the query term or terms, the date
10 of the query, the identifier of the personnel
11 conducting the query, and the written
12 statement of the specific factual basis re-
13 quired under clause (i).

14 “(D) AFFIRMATIVE ELECTION TO INCLUDE
15 SECTION 702 INFORMATION IN QUERIES.—Any
16 system of the Federal Bureau of Investigation
17 that stores unminimized contents or noncon-
18 tents obtained through acquisitions authorized
19 under subsection (a) together with contents or
20 noncontents obtained through other lawful
21 means shall be configured in a manner that re-
22 quires personnel of the Federal Bureau of In-
23 vestigation who are in compliance with the
24 training requirement under subparagraph (A)
25 to conduct such a query to affirmatively elect to

1 include such unminimized contents or noncon-
 2 tents obtained through acquisitions authorized
 3 under subsection (a) when running a query.”;
 4 and

5 (3) in paragraph (8), as so redesignated—

6 (A) by striking subparagraph (B) and in-
 7 serting the following:

8 “(B) The term ‘covered person’ means—

9 “(i) a United States person; or

10 “(ii) a person reasonably believed to
 11 be located in the United States—

12 “(I) at the time of the applicable
 13 query; or

14 “(II) at the time of the commu-
 15 nication or creation of the information
 16 subject to the applicable query.

17 “(C)(i) The term ‘covered query’ means a
 18 query that—

19 “(I) is conducted using 1 or more
 20 terms associated with 1 or more covered
 21 persons, including but not limited to per-
 22 sonally identifiable information;

23 “(II) is conducted in whole or in part
 24 for the purpose of detecting or retrieving

1 information of or concerning 1 or more
 2 covered persons; or

3 “(III) is conducted with specific rea-
 4 son to believe the query will detect or re-
 5 trieve information of or concerning 1 or
 6 more covered persons.

7 “(ii) Whether a query is a covered query
 8 shall be determined without regard to whether
 9 the information subject to the query has al-
 10 ready been detected or retrieved using a method
 11 other than a query described in clause (i).

12 “(D) The term ‘query’—

13 “(i) means the use of any technique,
 14 whether manual or automated, to detect or
 15 retrieve information obtained through ac-
 16 quisitions authorized under subsection (a)
 17 from within a system, collection, or assort-
 18 ment of information, or a subset thereof;
 19 and

20 “(ii) does not include the manual ob-
 21 servation of retrieved information.”.

22 (c) PROHIBITION ON WARRANTLESS ACCESS TO THE
 23 COMMUNICATIONS AND OTHER INFORMATION OF UNITED
 24 STATES PERSONS AND PERSONS LOCATED IN THE
 25 UNITED STATES.—Section 702(f) of the Foreign Intel-

1 ligence Surveillance Act of 1978 (50 U.S.C. 1881a(f)) is
 2 amended—

3 (1) in paragraph (1)(A) by inserting “and the
 4 limitations and requirements in paragraph (2)” after
 5 “Constitution of the United States”;

6 (2) by redesignating paragraph (4) as para-
 7 graph (5); and

8 (3) by striking paragraphs (2) and (3) and in-
 9 serting the following:

10 “(2) PROHIBITION ON WARRANTLESS ACCESS
 11 TO THE COMMUNICATIONS AND OTHER INFORMA-
 12 TION OF UNITED STATES PERSONS AND PERSONS
 13 LOCATED IN THE UNITED STATES.—

14 “(A) IN GENERAL.—Except as provided in
 15 subparagraph (B), no officer or employee of any
 16 agency that has access to unminimized commu-
 17 nications or information obtained through an
 18 acquisition under this section may access com-
 19 munications content, or information the com-
 20 pelled disclosure of which would require a prob-
 21 able cause warrant if sought for law enforce-
 22 ment purposes inside the United States, ac-
 23 quired under subsection (a) and returned in re-
 24 sponse to a covered query.

1 “(B) EXCEPTIONS FOR CONCURRENT AU-
2 THORIZATION, EXIGENT CIRCUMSTANCES, CON-
3 SENT, AND CERTAIN DEFENSIVE CYBERSECU-
4 RITY QUERIES.—

5 “(i) IN GENERAL.—Subparagraph (A)
6 shall not apply if—

7 “(I) the person to whom the cov-
8 ered query relates is the subject of an
9 order authorizing electronic surveil-
10 lance, a physical search, or an acquisi-
11 tion under section 105, section 304,
12 section 703, or section 704 of this Act
13 or a warrant issued pursuant to the
14 Federal Rules of Criminal Procedure
15 by a court of competent jurisdiction;

16 “(II)(aa) the person to whom the
17 covered query relates is the subject of
18 an emergency authorization author-
19 izing electronic surveillance, a physical
20 search, or an acquisition under section
21 105, section 304, section 703, or sec-
22 tion 704 of this Act;

23 “(bb) not later than 7 days after
24 the results of the covered query are
25 accessed, a description of the cir-

1 cumstances justifying the accessing of
2 the results of the covered query is
3 provided to the congressional intel-
4 ligence committees, the Committee on
5 the Judiciary of the House of Rep-
6 resentatives, and the Committee on
7 the Judiciary of the Senate;

8 “(cc) the Attorney General
9 makes or has made an application to
10 the Foreign Intelligence Surveillance
11 Court in accordance with section
12 105(e)(1)(D), section 304(e)(1)(D),
13 section 703(d)(1), or section
14 704(d)(1) of this Act; and

15 “(dd) in the event such applica-
16 tion is denied, the requirements of
17 section 105(e)(5), 304(e)(5), section
18 703(d)(4), or section 704(d)(4), as
19 applicable, are followed;

20 “(III) such person or, if such
21 person is incapable of providing con-
22 sent, a third party legally authorized
23 to consent on behalf of such person,
24 has provided consent for the access on
25 a case-by-case basis; or

1 “(IV)(aa) the communications
2 content or information is accessed and
3 used for the sole purpose of identi-
4 fying a potential victim or unwitting
5 conduit of malicious cyber activity
6 who is not a potential perpetrator of
7 such activity;

8 “(bb) other than for the purposes
9 described in item (aa), no communica-
10 tions content or other information de-
11 scribed in subparagraph (A) are
12 accessed or reviewed; and

13 “(cc) the accessing of query re-
14 sults is reported to the Foreign Intel-
15 ligence Surveillance Court.

16 “(ii) LIMITATIONS.—No communica-
17 tions content or information accessed
18 under clause (i)(II) or information derived
19 from such access may be used, received in
20 evidence, or otherwise disseminated in any
21 trial, hearing, or other proceeding in or be-
22 fore any court, grand jury, department, of-
23 fice, agency, regulatory body, legislative
24 committee, or other authority of the
25 United States, a State, or political subdivi-

1 sion thereof, except in a proceeding that
 2 arises from the circumstances to which the
 3 applicable emergency authorization relates.

4 “(iii) ASSESSMENT OF COMPLI-
 5 ANCE.—Not less frequently than annually,
 6 the Attorney General shall assess—

7 “(I) compliance with the require-
 8 ments under clause (i)(II)(cc); and

9 “(II) compliance with the re-
 10 quirements under clause (ii).

11 “(C) FOREIGN INTELLIGENCE PURPOSE.—

12 “(i) IN GENERAL.—Except as pro-
 13 vided in clause (ii) of this subparagraph,
 14 no officer or employee of any agency that
 15 has access to unminimized communications
 16 or information obtained through an acqui-
 17 sition under this section may conduct a
 18 covered query of information acquired
 19 under subsection (a) unless the query is
 20 reasonably likely to retrieve foreign intel-
 21 ligence information.

22 “(ii) EXCEPTIONS.—An officer or em-
 23 ployee of an agency that has access to
 24 unminimized communications or informa-
 25 tion obtained through an acquisition under

1 this section may conduct a covered query
2 of information acquired under this section
3 if—

4 “(I)(aa) the officer or employee
5 conducting the query has a reasonable
6 belief that—

7 “(AA) an emergency exists
8 involving an imminent threat of
9 death or serious bodily harm; and

10 “(BB) the query could rea-
11 sonably be expected to assist in
12 mitigating or eliminating that
13 threat to life or serious bodily
14 harm; and

15 “(bb) not later than 7 days after
16 the query is conducted, a description
17 of the query is provided to the For-
18 eign Intelligence Surveillance Court,
19 the congressional intelligence commit-
20 tees, the Committee on the Judiciary
21 of the House of Representatives, and
22 the Committee on the Judiciary of the
23 Senate; or

24 “(II) the query is necessary to
25 identify information that must be pro-

1 duced or preserved in connection with
2 a litigation matter or to fulfill dis-
3 covery obligations in a criminal matter
4 under the laws of the United States
5 or any State thereof.

6 “(D) NOTIFICATION AND CONSENT RE-
7 QUIREMENTS.—

8 “(i) APPROPRIATE CONGRESSIONAL
9 LEADERSHIP DEFINED.—In this subpara-
10 graph, the term ‘appropriate congressional
11 leadership’ means the following:

12 “(I) The chairs and ranking mi-
13 nority members of the congressional
14 intelligence committees.

15 “(II) The chair and ranking mi-
16 nority member of the Committee on
17 the Judiciary of the Senate and the
18 chair and ranking minority member of
19 Committee on the Judiciary of the
20 House of Representatives.

21 “(III) The Speaker and minority
22 leader of the House of Representa-
23 tives.

24 “(IV) The majority and minority
25 leaders of the Senate.

1 “(ii) NOTIFICATION REQUIREMENT
2 FOR CERTAIN FBI QUERIES.—

3 “(I) REQUIREMENT.—The Direc-
4 tor of the Federal Bureau of Inves-
5 tigation shall promptly notify appro-
6 priate congressional leadership of any
7 query conducted by the Federal Bu-
8 reau of Investigation using a query
9 term that is reasonably believed to be
10 the name or other personally identi-
11 fying information of a Member of
12 Congress, and shall also notify the
13 Member who is the subject of such
14 query.

15 “(II) NATIONAL SECURITY CON-
16 SIDERATIONS.—In submitting a notifi-
17 cation under subclause (I), the Direc-
18 tor shall give due regard to the pro-
19 tection of classified information,
20 sources and methods, and national se-
21 curity.

22 “(III) WAIVER.—

23 “(aa) IN GENERAL.—The
24 Director may waive a notification
25 required under subclause (I) if

1 the Director determines such no-
2 tification would impede an ongo-
3 ing national security or law en-
4 forcement investigation.

5 “(bb) TERMINATION.—A
6 waiver under item (aa) shall ter-
7 minate on the date the Director
8 determines the relevant notifica-
9 tion would not impede the rel-
10 evant national security or law en-
11 forcement investigation or on the
12 date that such investigation ends,
13 whichever is earlier.

14 “(iii) CONSENT REQUIRED FOR FBI
15 TO CONDUCT CERTAIN QUERIES FOR PUR-
16 POSE OF DEFENSIVE BRIEFING.—

17 “(I) CONSENT REQUIRED.—The
18 Federal Bureau of Investigation may
19 not, for the purpose of supplementing
20 the contents of a briefing on the de-
21 fense against a counterintelligence
22 threat to a Member of Congress, con-
23 duct a query using a query term that
24 is the name or restricted personal in-
25 formation (as such term is defined in

1 section 119 of title 18, United States
2 Code) of that Member unless—

3 “(aa) the Member provides
4 consent to the use of the query
5 term; or

6 “(bb) the Deputy Director
7 of the Federal Bureau of Inves-
8 tigation determines that exigent
9 circumstances exist sufficient to
10 justify the conduct of such query.

11 “(II) NOTIFICATION.—

12 “(aa) NOTIFICATION OF
13 CONSENT SOUGHT.—Not later
14 than 3 business days after sub-
15 mitting a request for consent
16 from a Member of Congress
17 under subclause (I), the Director
18 of the Federal Bureau of Inves-
19 tigation shall notify the appro-
20 priate congressional leadership,
21 regardless of whether the Mem-
22 ber provided such consent.

23 “(bb) NOTIFICATION OF EX-
24 CEPTION USED.—Not later than
25 3 business days after the conduct

1 of a query under subclause (I)
2 without consent on the basis of
3 the existence of exigent cir-
4 cumstances determined under
5 item (bb) of such subclause, the
6 Director of the Federal Bureau
7 of Investigation shall notify the
8 appropriate congressional leader-
9 ship.

10 “(III) RULE OF CONSTRUC-
11 TION.—Nothing in this clause may be
12 construed as—

13 “(aa) applying to matters
14 outside of the scope of the brief-
15 ing on the defense against a
16 counterintelligence threat to be
17 provided or supplemented under
18 subclause (I); or

19 “(bb) limiting the lawful in-
20 vestigative activities of the Fed-
21 eral Bureau of Investigation
22 other than supplementing the
23 contents of a briefing on the de-
24 fense against a counterintel-

1 ligence threat to a Member of
2 Congress.

3 “(3) DOCUMENTATION.—No officer or employee
4 of any agency that has access to unminimized com-
5 munications or information obtained through an ac-
6 quisition under this section may access communica-
7 tions content, or information the compelled disclo-
8 sure of which would require a probable cause war-
9 rant if sought for law enforcement purposes inside
10 the United States, returned in response to a covered
11 query unless an electronic record is created that in-
12 cludes a statement of facts showing that the access
13 is authorized pursuant to an exception specified in
14 paragraph (2)(B).

15 “(4) QUERY RECORD SYSTEM.—The head of
16 each agency that has access to unminimized commu-
17 nications or information obtained through an acqui-
18 sition under this section shall ensure that a system,
19 mechanism, or business practice is in place to main-
20 tain the records described in paragraph (3). Not
21 later than 90 days after the date of enactment of
22 the SAFE Act, the head of each agency that has ac-
23 cess to unminimized communications or information
24 obtained through an acquisition under this section

1 shall report to Congress on its compliance with this
 2 procedure.”.

3 (d) CONFORMING AMENDMENTS.—

4 (1) Section 603(b)(2) of the Foreign Intel-
 5 ligence Surveillance Act of 1978 (50 U.S.C.
 6 1873(b)(2)) is amended, in the matter preceding
 7 subparagraph (A), by striking “, including pursuant
 8 to subsection (f)(2) of such section,”.

9 (2) Section 706(a)(2)(A)(i) of the Foreign In-
 10 telligence Surveillance Act of 1978 (50 U.S.C.
 11 1881e(a)(2)(A)(i)) is amended by striking “obtained
 12 an order of the Foreign Intelligence Surveillance
 13 Court to access such information pursuant to section
 14 702(f)(2)” and inserting “accessed such information
 15 in accordance with section 702(b)(2)”.

16 **SEC. 102. ANNUAL REPORTS.**

17 (a) IN GENERAL.—Section 707 of the Foreign Intel-
 18 ligence Surveillance Act of 1978 (50 U.S.C. 1881f) is
 19 amended by adding at the end the following:

20 “(c) ANNUAL REPORTS.—

21 “(1) IN GENERAL.—The Attorney General, in
 22 consultation with the Director of National Intel-
 23 ligence, shall submit to the congressional intelligence
 24 committees, the Committee on the Judiciary of the
 25 Senate, and the Committee on the Judiciary of the

1 House of Representatives an annual report, which
2 shall include, for that year, disaggregated by each
3 agency that conducts queries of information acquired
4 under section 702, the following information:

5 “(A) The total number of covered queries
6 (as defined in section 702(f)(8)) conducted of
7 information acquired under section 702.

8 “(B) The number of times an officer or
9 employee of the United States accessed commu-
10 nications contents (as defined in section
11 2510(8) of title 18, United States Code) or in-
12 formation the compelled disclosure of which
13 would require a probable cause warrant if
14 sought for law enforcement purposes in the
15 United States, returned in response to such
16 queries.

17 “(C) The number of applications for orders
18 described in subclause (I) of section
19 702(f)(2)(B)(i) with respect to a person for
20 which communications contents or information
21 relating to such person were accessed under
22 such subclause and the number of such orders
23 granted.

24 “(D) The number of times an exception
25 under subclause (II), (III), or (IV) of section

1 702(f)(2)(B)(i) was asserted, disaggregated by
2 the subclause under which an exception was as-
3 serted.

4 “(E) The number of times that 2 or more
5 approved queries were conducted together,
6 through the use of batch job technology, any
7 successor tool, or any other batch query meth-
8 od.

9 “(F) The number of queries run by an
10 agency with access to unminimized communica-
11 tions or information obtained through an acqui-
12 sition under section 702 run at the request of
13 or on behalf of 1 or more other agencies that
14 do not have such access, broken down by the
15 agency that ran the query, the agency for whom
16 the query was run, and the date of the query.

17 “(2) PUBLIC AVAILABILITY.—Subject to declassi-
18 fication review by the Attorney General and the
19 Director of National Intelligence, each annual report
20 submitted pursuant to paragraph (1) shall be made
21 publicly available during April of each year and in-
22 clude information relating to the previous calendar
23 year.”.

1 (b) REPEAL OF SUPERSEDED REPORTING REQUIRE-
 2 MENT.—Section 603 of the Foreign Intelligence Surveil-
 3 lance Act of 1978 (50 U.S.C. 1873) is amended—

4 (1) by striking subsection (f); and

5 (2) by redesignating subsection (g) as sub-
 6 section (f).

7 **SEC. 103. ACCOUNTABILITY AND REPORTING PROCEDURES**
 8 **FOR COMPLIANCE VIOLATIONS RELATING TO**
 9 **QUERIES CONDUCTED BY THE FEDERAL BU-**
 10 **REAU OF INVESTIGATION.**

11 (a) IN GENERAL.—Title VII of the Foreign Intel-
 12 ligence Surveillance Act of 1978 (50 U.S.C. 1881 et seq.)
 13 is amended by adding at the end the following:

14 **“SEC. 710. ACCOUNTABILITY PROCEDURES FOR INCIDENTS**
 15 **RELATING TO QUERIES CONDUCTED BY THE**
 16 **FEDERAL BUREAU OF INVESTIGATION.**

17 “(a) IN GENERAL.—The Director of the Federal Bu-
 18 reau of Investigation shall establish procedures to hold
 19 employees of the Federal Bureau of Investigation account-
 20 able for violations of law, guidance, and procedure gov-
 21 erning queries of information acquired pursuant to section
 22 702.

23 “(b) ELEMENTS.—The procedures established under
 24 subsection (a) shall include the following:

1 “(1) Centralized tracking of individual employee
2 performance incidents involving violations of law,
3 guidance, and procedure described in subsection (a),
4 over time.

5 “(2) Escalating consequences for such inci-
6 dents, including—

7 “(A) consequences for initial incidents, in-
8 cluding, at a minimum—

9 “(i) suspension of access to informa-
10 tion acquired under this Act pending reme-
11 dial action; and

12 “(ii) documentation of the incident in
13 the personnel file of each employee respon-
14 sible for the violation; and

15 “(B) consequences for subsequent inci-
16 dents, including, at a minimum—

17 “(i) possible indefinite suspension of
18 access to information acquired under this
19 Act;

20 “(ii) reassignment of each employee
21 responsible for the violation; and

22 “(iii) referral of the incident to the
23 Inspection Division of the Federal Bureau
24 of Investigation for review of potentially
25 reckless conduct.

1 “(3) Clarification of requirements for referring
2 intentional misconduct and reckless conduct to the
3 Inspection Division of the Federal Bureau of Inves-
4 tigation for investigation and disciplinary action by
5 the Office of Professional Responsibility of the Fed-
6 eral Bureau of Investigation.”.

7 (b) CLERICAL AMENDMENT.—The table of contents
8 for the Foreign Intelligence Surveillance Act of 1978 (50
9 U.S.C. 1801 et seq.) is amended by inserting after the
10 item relating to section 709 the following:

 “Sec. 710. Accountability procedures for incidents relating to queries conducted
 by the Federal Bureau of Investigation.”.

11 (c) REPORT REQUIRED.—

12 (1) INITIAL REPORT.—Not later than 180 days
13 after the date of enactment of this Act, the Director
14 of the Federal Bureau of Investigation shall submit
15 to the Committee on the Judiciary of the House of
16 Representatives, the Committee on the Judiciary of
17 the Senate, and the congressional intelligence com-
18 mittees (as such term is defined in section 801 of
19 the Foreign Intelligence Surveillance Act of 1978
20 (50 U.S.C. 1885)) a report detailing the procedures
21 established under section 710 of the Foreign Intel-
22 ligence Surveillance Act of 1978, as added by sub-
23 section (a).

1 (2) ANNUAL REPORT.—Not later than 1 year
2 after the date of enactment of this Act, and annually
3 thereafter, the Federal Bureau of Investigation shall
4 submit to the Committee on the Judiciary of the
5 House of Representatives, the Committee on the Ju-
6 diciary of the Senate, and the congressional intel-
7 ligence committees (as such term is defined in sec-
8 tion 801 of the Foreign Intelligence Surveillance Act
9 of 1978 (50 U.S.C. 1885)) a report on any discipli-
10 nary actions taken pursuant to the procedures estab-
11 lished under section 710 of the Foreign Intelligence
12 Surveillance Act of 1978, as added by subsection
13 (a), including a description of the circumstances sur-
14 rounding each such disciplinary action, and the re-
15 sults of each such disciplinary action.

16 (3) FORM.—The reports required under para-
17 graphs (1) and (2) shall be submitted in unclassified
18 form, but may include a classified annex to the ex-
19 tent necessary to protect sources and methods.

20 (d) ANNUAL REPORTS.—Paragraph (5) of section
21 702(f) of the Foreign Intelligence Surveillance Act of 1978
22 (50 U.S.C. 1881a(f)), as redesignated by section 101(c)(2)
23 of this Act, is amended—

1 (1) by redesignating subparagraphs (A), (B),
 2 and (C) as clauses (i), (ii), and (iii), respectively,
 3 and adjusting the margin accordingly;

4 (2) by striking “The Director” and inserting
 5 the following:

6 “(A) IN GENERAL.—The Director”; and

7 (3) by adding at the end the following:

8 “(B) ANNUAL REPORTS.—The Director of
 9 the Federal Bureau of Investigation shall sub-
 10 mit to the congressional intelligence commit-
 11 tees, the Committee on the Judiciary of the
 12 Senate, and the Committee on the Judiciary of
 13 the House of Representatives an annual report
 14 on the actions taken under the minimum ac-
 15 countability standards issued under subpara-
 16 graph (A).”.

17 (e) RESTRICTION ON CERTAIN INFORMATION AVAIL-
 18 ABLE TO THE FEDERAL BUREAU OF INVESTIGATION.—
 19 Section 702(n)(2) of the Foreign Intelligence Surveillance
 20 Act of 1978 (50 U.S.C. 1881a(n)(2)) is amended by in-
 21 serting “the Committee on the Judiciary of the Senate,
 22 the Committee on the Judiciary of the House of Rep-
 23 resentatives,” after “the congressional intelligence com-
 24 mittees,”.

1 **SEC. 104. PROHIBITION ON REVERSE TARGETING OF**
 2 **UNITED STATES PERSONS AND PERSONS LO-**
 3 **CATED IN THE UNITED STATES.**

4 Section 702 of the Foreign Intelligence Surveillance
 5 Act of 1978 (50 U.S.C. 1881a) is amended—

6 (1) in subsection (b)(2), by striking “if the pur-
 7 pose of such acquisition is to target a particular,
 8 known person reasonably believed to be in the
 9 United States;” and inserting “if a purpose of such
 10 acquisition is to target 1 or more United States per-
 11 sons or persons reasonably believed to be located in
 12 the United States at the time of acquisition or com-
 13 munication;”;

14 (2) in subsection (d)(1), by amending subpara-
 15 graph (A) to read as follows:

16 “(A) ensure that—

17 “(i) any acquisition authorized under
 18 subsection (a) is limited to targeting per-
 19 sons reasonably believed to be non-United
 20 States persons located outside the United
 21 States; and

22 “(ii) targeting 1 or more United
 23 States persons or persons reasonably be-
 24 lieved to be in the United States at the
 25 time of acquisition or communication is not
 26 a purpose of an acquisition; and”;

1 (3) in subsection (h)(2)(A)(i), by amending sub-
2 clause (I) to read as follows:

3 “(I) ensure that—

4 “(aa) an acquisition author-
5 ized under subsection (a) is lim-
6 ited to targeting persons reason-
7 ably believed to be non-United
8 States persons located outside
9 the United States; and

10 “(bb) a purpose of an acqui-
11 sition is not to target 1 or more
12 United States persons or persons
13 reasonably believed to be in the
14 United States at the time of ac-
15 quisition or communication;
16 and”; and

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

19 “(i) ensure that—

20 “(I) an acquisition authorized
21 under subsection (a) is limited to tar-
22 geting persons reasonably believed to
23 be non-United States persons located
24 outside the United States; and

1 “(II) a purpose of an acquisition
 2 is not to target 1 or more United
 3 States persons or persons reasonably
 4 believed to be in the United States at
 5 the time of acquisition or communica-
 6 tion; and”.

7 **SEC. 105. FISA COURT REVIEW OF TARGETING DECISIONS.**

8 Section 702 of the Foreign Intelligence Surveillance
 9 Act of 1978 (50 U.S.C. 1881a) is amended—

10 (1) in subsection (h)(2)—

11 (A) in subparagraph (D)(ii), by striking
 12 “and” at the end;

13 (B) in subparagraph (E), by striking the
 14 period at the end and inserting “; and”; and

15 (C) by adding at the end the following:

16 “(F) include a random sample of targeting
 17 decisions and supporting written justifications
 18 from the prior year, using a sample size and
 19 methodology that has been approved by the
 20 Foreign Intelligence Surveillance Court.”; and

21 (2) in subsection (j)(1)—

22 (A) by striking “subsection (g)” each place
 23 it appears and inserting “subsection (h)”; and

24 (B) in subparagraph (A), as amended by
 25 subparagraph (A) of this paragraph, by insert-

ing “, including reviewing the random sample of
targeting decisions and written justifications
submitted under subsection (h)(2)(F),” after
“subsection (h)”.

SEC. 106. SUNSET OF CHANGES TO DEFINITION OF ELECTRONIC COMMUNICATION SERVICE PROVIDER.

Effective on December 31, 2026, the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended—

(1) in section 701(b)(4) (50 U.S.C. 1881(b)(4))—

(A) in subparagraph (D), by adding “or” at the end;

(B) by striking subparagraph (E);

(C) by redesignating subparagraph (F) as subparagraph (E); and

(D) in subparagraph (E), as so redesignated—

(i) by striking “custodian,”; and

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

(2) in section 801(6) (50 U.S.C. 1885(6))—

(A) by striking subparagraph (E);

1 (B) by redesignating subparagraphs (F)
 2 and (G) as subparagraphs (E) and (F), respec-
 3 tively;

4 (C) in subparagraph (E), as so redesign-
 5 nated, by adding “or” at the end; and

6 (D) in subparagraph (F), as so redesign-
 7 nated—

8 (i) by striking “custodian,”; and

9 (ii) by striking “(E), or (F)” and in-
 10 serting “or (E)”.

11 **SEC. 107. LIMITATION ON DIRECTIVES UNDER FOREIGN IN-**
 12 **TELLIGENCE SURVEILLANCE ACT OF 1978 RE-**
 13 **LATING TO CERTAIN ELECTRONIC COMMU-**
 14 **NICATION SERVICE PROVIDERS.**

15 (a) IN GENERAL.—Section 702(i) of the Foreign In-
 16 telligence Surveillance Act of 1978 (50 U.S.C. 1881a(i))
 17 is amended by adding at the end the following:

18 “(7) LIMITATION RELATING TO CERTAIN ELEC-
 19 TRONIC COMMUNICATION SERVICE PROVIDERS.—

20 “(A) DEFINITIONS.—In this paragraph:

21 “(i) APPROPRIATE COMMITTEES OF
 22 CONGRESS.—The term ‘appropriate com-
 23 mittees of Congress’ means—

24 “(I) the congressional intelligence
 25 committees;

1 “(II) the Committee on the Judi-
2 ciary of the Senate; and

3 “(III) the Committee on the Ju-
4 diciary of the House of Representa-
5 tives.

6 “(ii) COVERED ELECTRONIC COMMU-
7 NICATION SERVICE PROVIDER.—

8 “(I) IN GENERAL.—Subject to
9 subclause (II), the term ‘covered elec-
10 tronic communication service provider’
11 means—

12 “(aa) a service provider de-
13 scribed in section 701(b)(4)(E);

14 “(bb) a custodian of an enti-
15 ty as defined in section
16 701(b)(4)(F); or

17 “(cc) an officer, employee,
18 or agent of a service provider de-
19 scribed in section 701(b)(4)(E).

20 “(II) EXCLUSION.—The term
21 ‘covered electronic communication
22 service provider’ does not include—

23 “(aa) an electronic commu-
24 nication service provider de-
25 scribed in subparagraph (A), (B),

1 (C), or (D) of section 701(b)(4);
2 or

3 “(bb) an officer, employee,
4 or agent of an electronic commu-
5 nication service provider de-
6 scribed in subparagraph (A), (B),
7 (C), or (D) of section 701(b)(4),
8 to the extent that the electronic com-
9 munication service provider is pro-
10 viding the United States Government
11 with information, facilities, or assist-
12 ance pursuant to such subparagraphs.

13 “(iii) COVERED OPINIONS.—The term
14 ‘covered opinions’ means the opinions of
15 the Foreign Intelligence Surveillance Court
16 and the Foreign Intelligence Surveillance
17 Court of Review authorized for public re-
18 lease on August 23, 2023 (Opinion and
19 Order, In re Petition to Set Aside or Mod-
20 ify Directive Issued to [REDACTED], No.
21 [REDACTED], (FISA Ct. [REDACTED]
22 2022) (Contreras J.); Opinion, In re Peti-
23 tion to Set Aside or Modify Directive
24 Issued to [REDACTED], No. [RE-
25 DACTED], (FISA Ct. Rev. [RE-

1 DACTED] 2023) (Sentelle, J.; Higginson,
2 J.; Miller J.)).

3 “(B) LIMITATION.—A directive may not be
4 issued under paragraph (1) to a covered elec-
5 tronic communication service provider unless
6 the covered electronic communication service
7 provider is a provider of the type of service at
8 issue in the covered opinions.

9 “(C) DECLASSIFICATION REVIEW RE-
10 QUIRED.—

11 “(i) IN GENERAL.—Not later than
12 180 days after the date of enactment of
13 the SAFE Act, the Director of National
14 Intelligence, in consultation with the Attor-
15 ney General, shall complete a declassifica-
16 tion review in accordance with section 3 of
17 Executive Order 13526 (50 U.S.C. 3161
18 note; relating to classified national security
19 information), or any successor order, (in
20 this subparagraph referred to as ‘Executive
21 Order 13526’) and, consistent with that
22 review, make publicly available to the
23 greatest extent practicable the type of serv-
24 ice provider and services at issue in the
25 covered opinions.

1 “(ii) SPECIFIC INQUIRY.—In con-
 2 ducting the review required under clause
 3 (i), the Director of National Intelligence
 4 and the Attorney General shall deter-
 5 mine—

6 “(I) whether the information de-
 7 scribed in clause (i) continues to meet
 8 the requirements for classification set
 9 forth in Executive Order 13526; and

10 “(II) if the information described
 11 in clause (i) continues to meet the re-
 12 quirements for classification set forth
 13 in Executive Order 13526, whether
 14 the information should nonetheless be
 15 declassified pursuant to section 3.1(d)
 16 of Executive Order 13526.

17 “(iii) FACTORS.—In making a deter-
 18 mination under subclause (II) of clause
 19 (ii), the Director of National Intelligence
 20 and the Attorney General shall consider—

21 “(I) the public interest served by
 22 ensuring that laws are public and
 23 transparent; and

24 “(II) the fact that the type of
 25 service provider or services at issue in

1 the covered opinions have been the
2 subject of public disclosures.

3 “(D) REQUIREMENTS FOR DIRECTIVES TO
4 COVERED ELECTRONIC COMMUNICATION SERV-
5 ICE PROVIDERS.—

6 “(i) IN GENERAL.—Subject to clause
7 (ii), any directive issued under paragraph
8 (1) on or after the date of the enactment
9 of the SAFE Act to a covered electronic
10 communication service provider that is not
11 prohibited by subparagraph (B) of this
12 paragraph shall include a summary de-
13 scription of the services at issue in the cov-
14 ered opinions.

15 “(ii) DUPLICATE SUMMARIES NOT RE-
16 QUIRED.—A directive need not include a
17 summary description of the services at
18 issue in the covered opinions if such sum-
19 mary was included in a prior directive
20 issued to the covered electronic commu-
21 nication service provider and the summary
22 has not materially changed.

23 “(E) FOREIGN INTELLIGENCE SURVEIL-
24 LANCE COURT NOTIFICATION AND REVIEW.—

25 “(i) NOTIFICATION.—

1 “(I) IN GENERAL.—Subject to
2 subclause (II), on or after the date of
3 the enactment of the SAFE Act, each
4 time the Attorney General and the Di-
5 rector of National Intelligence serve a
6 directive under paragraph (1) to a
7 covered electronic communication
8 service provider that is not prohibited
9 by subparagraph (B) and each time
10 the Attorney General and the Director
11 materially change a directive under
12 paragraph (1) served on a covered
13 electronic communication service pro-
14 vider that is not prohibited by sub-
15 paragraph (B), the Attorney General
16 shall provide the directive to the For-
17 eign Intelligence Surveillance Court
18 on or before the date that is 7 days
19 after the date on which the Attorney
20 General and the Director served the
21 directive, along with a description of
22 the covered electronic communication
23 service provider to whom the directive
24 is issued and the services at issue.

1 “(II) DUPLICATION NOT RE-
2 QUIRED.—The Attorney General does
3 not need to provide a directive or de-
4 scription to the Foreign Intelligence
5 Surveillance Court under subclause (I)
6 if a directive and description con-
7 cerning the covered electronic commu-
8 nication service provider was pre-
9 viously provided to the Court and the
10 directive or description has not mate-
11 rially changed.

12 “(ii) ADDITIONAL INFORMATION.—As
13 soon as feasible and not later than the ini-
14 tiation of collection, the Attorney General
15 shall, for each directive described in clause
16 (i), provide the Foreign Intelligence Sur-
17 veillance Court a summary description of
18 the type of equipment to be accessed, the
19 nature of the access, and the form of as-
20 sistance required pursuant to the directive.

21 “(iii) REVIEW.—

22 “(I) IN GENERAL.—The Foreign
23 Intelligence Surveillance Court may
24 review a directive received by the
25 Court under clause (i) to determine

1 whether the directive is consistent
2 with subparagraph (B) and affirm,
3 modify, or set aside the directive.

4 “(II) NOTICE OF INTENT TO RE-
5 VIEW.—Not later than 7 days after
6 the date on which the Court receives
7 information under clause (ii) with re-
8 spect to a directive, the Court shall
9 provide notice to the Attorney General
10 and cleared counsel for the covered
11 electronic communication service pro-
12 vider indicating whether the Court in-
13 tends to undertake a review under
14 subclause (I) of this clause.

15 “(III) COMPLETION OF RE-
16 VIEWS.—In a case in which the Court
17 provides notice under subclause (II)
18 indicating that the Court intends to
19 review a directive under subclause (I),
20 the Court shall, not later than 30
21 days after the date on which the
22 Court provides notice under subclause
23 (II) with respect to the directive, com-
24 plete the review.

25 “(F) CONGRESSIONAL OVERSIGHT.—

1 “(i) NOTIFICATION.—

2 “(I) IN GENERAL.—Subject to
3 subclause (II), on or after the date of
4 the enactment of the SAFE Act, each
5 time the Attorney General and the Di-
6 rector of National Intelligence serve a
7 directive under paragraph (1) on a
8 covered electronic communication
9 service provider that is not prohibited
10 by subparagraph (B) and each time
11 the Attorney General and the Director
12 materially change a directive under
13 paragraph (1) served on a covered
14 electronic communication service pro-
15 vider that is not prohibited by sub-
16 paragraph (B), the Attorney General
17 shall submit to the appropriate com-
18 mittees of Congress the directive on or
19 before the date that is 7 days after
20 the date on which the Attorney Gen-
21 eral and the Director serve the direc-
22 tive, along with a description of the
23 covered electronic communication
24 service provider to whom the directive
25 is issued and the services at issue.

1 “(II) DUPLICATION NOT RE-
2 QUIRED.—The Attorney General does
3 not need to submit a directive or de-
4 scription to the appropriate commit-
5 tees of Congress under subclause (I)
6 if a directive and description con-
7 cerning the covered electronic commu-
8 nication service provider was pre-
9 viously submitted to the appropriate
10 committees of Congress and the direc-
11 tive or description has not materially
12 changed.

13 “(ii) ADDITIONAL INFORMATION.—As
14 soon as feasible and not later than the ini-
15 tiation of collection, the Attorney General
16 shall, for each directive described in clause
17 (i), provide the appropriate committees of
18 Congress a summary description of the
19 type of equipment to be accessed, the na-
20 ture of the access, and the form of assist-
21 ance required pursuant to the directive.

22 “(iii) REPORTING.—

23 “(I) QUARTERLY REPORTS.—Not
24 later than 90 days after the date of
25 the enactment of the SAFE Act and

1 not less frequently than once each
2 quarter thereafter, the Attorney Gen-
3 eral shall submit to the appropriate
4 committees of Congress a report on
5 the number of directives served, dur-
6 ing the period covered by the report,
7 under paragraph (1) to a covered elec-
8 tronic communication service provider
9 and the number of directives provided
10 during the same period to the Foreign
11 Intelligence Surveillance Court under
12 subparagraph (E)(i).

13 “(II) FORM OF REPORTS.—Each
14 report submitted pursuant to sub-
15 clause (I) shall be submitted in un-
16 classified form, but may include a
17 classified annex.

18 “(III) SUBMISSION OF COURT
19 OPINIONS.—Not later than 45 days
20 after the date on which the Foreign
21 Intelligence Surveillance Court or the
22 Foreign Intelligence Surveillance
23 Court of Review issues an opinion re-
24 lating to a directive issued to a cov-
25 ered electronic communication service

1 provider under paragraph (1), the At-
 2 torney General shall submit to the ap-
 3 propriate committees of Congress a
 4 copy of the opinion.”.

5 (b) SUNSET.—Effective on December 31, 2026, sec-
 6 tion 702(i) of the Foreign Intelligence Surveillance Act of
 7 1978 (50 U.S.C. 1881a(i)), as amended by this section,
 8 is amended by striking paragraph (7).

9 **SEC. 108. EXTENSION OF TITLE VII OF FISA; EXPIRATION**
 10 **OF FISA AUTHORITIES; EFFECTIVE DATES.**

11 (a) EFFECTIVE DATES.—Section 403(b) of the FISA
 12 Amendments Act of 2008 (Public Law 110–261; 122 Stat.
 13 2474) is amended—

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

15 (A) by striking “two years after the date
 16 of enactment of the Reforming Intelligence and
 17 Securing America Act” and inserting “on April
 18 20, 2028”; and

19 (B) by striking “, as amended by section
 20 101(a) and by the FISA Amendments Reau-
 21 thorization Act of 2017 and the Reforming In-
 22 telligence and Securing America Act,” and in-
 23 serting “, as most recently amended,”; and

24 (2) in paragraph (2) (18 U.S.C. 2511 note), in
 25 the matter preceding subparagraph (A), by striking

1 “two years after the date of enactment of the Re-
2 forming Intelligence and Securing America Act” and
3 inserting “on April 20, 2028”.

4 (b) CONFORMING AMENDMENTS.—Section 404(b) of
5 the FISA Amendments Act of 2008 (Public Law 110–261;
6 122 Stat. 2476), is amended—

7 (1) in paragraph (1)—

8 (A) in the heading, by striking “TWO
9 YEARS AFTER THE DATE OF ENACTMENT OF
10 THE REFORMING INTELLIGENCE AND SECURING
11 AMERICA ACT” and inserting “APRIL 20, 2028”;
12 and

13 (B) by striking “, as amended by section
14 101(a) and by the FISA Amendments Reau-
15 thorization Act of 2017 and the Reforming In-
16 telligence and Securing America Act,” and in-
17 serting “, as most recently amended,”;

18 (2) in paragraph (2), by striking “, as amended
19 by section 101(a) and by the FISA Amendments Re-
20 authorization Act of 2017 and the Reforming Intel-
21 ligence and Securing America Act,” and inserting “,
22 as most recently amended,”; and

23 (3) in paragraph (4)—

24 (A) by striking “, as added by section
25 101(a) and amended by the FISA Amendments

1 Reauthorization Act of 2017 and the Reforming
 2 Intelligence and Securing America Act,” both
 3 places it appears and inserting “, as added by
 4 section 101(a) and as most recently amended,”;
 5 and

6 (B) by striking “, as amended by section
 7 101(a) and by the FISA Amendments Reau-
 8 thorization Act of 2017 and the Reforming In-
 9 telligence and Securing America Act,” both
 10 places it appears and inserting “, as most re-
 11 cently amended,”.

12 **TITLE II—ADDITIONAL RE-**
 13 **FORMS RELATING TO ACTIVI-**
 14 **TIES UNDER THE FOREIGN**
 15 **INTELLIGENCE SURVEIL-**
 16 **LANCE ACT OF 1978**

17 **SEC. 201. REQUIRED DISCLOSURE OF INFORMATION AND**
 18 **LIMITS ON USE OF CERTAIN INFORMATION**
 19 **AND ON ISSUANCE OF ORDERS.**

20 (a) REQUIRED DISCLOSURE OF RELEVANT INFORMA-
 21 TION IN FOREIGN INTELLIGENCE SURVEILLANCE ACT OF
 22 1978 APPLICATIONS.—

23 (1) IN GENERAL.—The Foreign Intelligence
 24 Surveillance Act of 1978 (50 U.S.C. 1801 et seq.)
 25 is amended by adding at the end the following:

1 **“TITLE IX—REQUIRED DISCLO-**
 2 **SURE OF RELEVANT INFOR-**
 3 **MATION**

4 **“SEC. 901. DISCLOSURE OF RELEVANT INFORMATION.**

5 “The Attorney General or any other Federal officer
 6 or employee making an application for a court order under
 7 this Act shall provide the court with all information in the
 8 possession of the Government that is material to deter-
 9 mining whether the application satisfies the applicable re-
 10 quirements under this Act, including any exculpatory in-
 11 formation.”.

12 (2) COLLECTION OF COMMUNICATIONS UNDER
 13 SECTION 702.—Section 702(h)(2) of the Foreign In-
 14 telligence Surveillance Act of 1978 (50 U.S.C.
 15 1881a(h)(2)) is amended—

16 (A) in subparagraph (D)(ii), by striking
 17 “and” at the end;

18 (B) in subparagraph (E), by striking the
 19 period at the end and inserting “; and”; and

20 (C) by adding at the end the following:

21 “(F) attest that, to the best of the knowl-
 22 edge of the person making the certification, the
 23 Attorney General and the Director of National
 24 Intelligence have been apprised of all informa-

tion in the possession of the Government that
might reasonably—

“(i) call into question the accuracy of
the certification or the reasonableness of
any assessment in the certification con-
ducted by the department or agency on
whose behalf the application is made; or

“(ii) otherwise raise doubts with re-
spect to the findings that are required to
be made under subsection (j).”.

(3) CLERICAL AMENDMENTS.—

(A) The table of contents for the Foreign
Intelligence Surveillance Act of 1978 is amend-
ed by adding at the end the following:

“TITLE IX—REQUIRED DISCLOSURE OF RELEVANT
INFORMATION

“Sec. 901. Disclosure of relevant information.”.

(B) Section 104(a)(13) of the Foreign In-
telligence Surveillance Act of 1978 (50 U.S.C.
1804(a)(13)) is repealed.

(C) Section 10(a)(7) of the Reforming In-
telligence and Securing America Act (50 U.S.C.
1804 note) is repealed.

(b) CERTIFICATION REGARDING ACCURACY PROCE-
DURES.—

1 (1) CERTIFICATION REGARDING ACCURACY PRO-
 2 CEDURES.—Title IX of the Foreign Intelligence Sur-
 3 veillance Act of 1978, as added by subsection (a) of
 4 this section, is amended by adding at the end the
 5 following:

6 **“SEC. 902. CERTIFICATION REGARDING ACCURACY PROCE-**
 7 **DURES.**

8 “(a) DEFINITION OF ACCURACY PROCEDURES.—In
 9 this section, the term ‘accuracy procedures’ means specific
 10 procedures, adopted by the Attorney General, to ensure
 11 that an application for a court order under this Act, in-
 12 cluding any application for renewal of an existing order,
 13 is accurate and complete, including procedures that en-
 14 sure, at a minimum, that—

15 “(1) the application reflects all information that
 16 might reasonably call into question the accuracy of
 17 the information or the reasonableness of any assess-
 18 ment in the application, or otherwise raises doubts
 19 about or contradicts the requested findings;

20 “(2) the application reflects all material infor-
 21 mation that might reasonably call into question the
 22 reliability and reporting of any information from a
 23 confidential human source that is used in the appli-
 24 cation;

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

3 “(4) the applicant coordinates with the appro-
4 priate elements of the intelligence community (as de-
5 fined in section 3 of the National Security Act of
6 1947 (50 U.S.C. 3003)), concerning any prior or ex-
7 isting relationship with the target of any surveil-
8 lance, search, or other means of investigation, and
9 discloses any such relationship in the application;

10 “(5) before any application targeting a United
11 States person (as defined in section 101) is made,
12 the applicant Federal officer shall document that the
13 officer has collected and reviewed for accuracy and
14 completeness supporting documentation for each fac-
15 tual assertion in the application; and

16 “(6) the applicant Federal agency establish
17 compliance and auditing mechanisms to address, on
18 an annual basis, the efficacy of the accuracy proce-
19 dures that have been adopted and report such find-
20 ings to the Attorney General.

21 “(b) STATEMENT AND CERTIFICATION OF ACCURACY
22 PROCEDURES.—Any Federal officer making an applica-
23 tion for a court order under this Act shall include with
24 the application—

1 “(1) a description of the accuracy procedures
2 employed by the officer or the officer’s designee; and

3 “(2) a certification that the officer or the offi-
4 cer’s designee has collected and reviewed for accu-
5 racy and completeness—

6 “(A) supporting documentation for each
7 factual assertion contained in the application;

8 “(B) all information that might reasonably
9 call into question the accuracy of the informa-
10 tion or the reasonableness of any assessment in
11 the application, or otherwise raises doubts
12 about the requested findings; and

13 “(C) all material information that might
14 reasonably call into question the reliability and
15 reporting of any information from any confiden-
16 tial human source that is used in the applica-
17 tion.

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

1 (2) TECHNICAL AMENDMENT.—The table of
 2 contents for the Foreign Intelligence Surveillance
 3 Act of 1978, as amended by subsection (a) of this
 4 section, is amended by adding at the end the fol-
 5 lowing:

“Sec. 902. Certification regarding accuracy procedures.”.

6 (c) PROHIBITION ON USE OF CERTAIN INFORMA-
 7 TION.—

8 (1) IN GENERAL.—Section 104 of the Foreign
 9 Intelligence Surveillance Act of 1978 (50 U.S.C.
 10 1804) is amended by adding at the end the fol-
 11 lowing:

12 “(e) The statement of facts and circumstances under
 13 subsection (a)(3) may only include information obtained
 14 from the content of a media source or information gath-
 15 ered by a political campaign if—

16 “(1) such information is disclosed in the appli-
 17 cation as having been so obtained or gathered;

18 “(2) with regard to information gathered from
 19 the content of a media source, the application in-
 20 cludes an explanation of the investigative techniques
 21 used to corroborate the information; and

22 “(3) with regard to information gathered by a
 23 political campaign, such information is not the sole
 24 source of the information used to justify the appli-
 25 cant’s belief described in subsection (a)(3).”.

1 (2) TECHNICAL AND CONFORMING AMEND-
2 MENTS.—The Foreign Intelligence Surveillance Act
3 of 1978 (50 U.S.C. 1801 et seq.) is amended—

4 (A) in section 104(a)(6) (50 U.S.C.
5 1804(a)(6))—

6 (i) in subparagraph (D), by striking
7 the semicolon at the end and inserting “;
8 and”;

9 (ii) in subparagraph (E)(ii), by strik-
10 ing “and” at the end; and

11 (iii) by striking subparagraphs (F)
12 and (G); and

13 (B) in section 303(a)(6) (50 U.S.C.
14 1823(a)(6))—

15 (i) in subparagraph (D), by striking
16 the semicolon at the end and inserting “;
17 and”;

18 (ii) in subparagraph (E), by striking
19 “and” at the end; and

20 (iii) by striking subparagraphs (F)
21 and (G).

22 (d) LIMITATION ON ISSUANCE OF ORDER.—Section
23 105(a) of the Foreign Intelligence Surveillance Act of
24 1978 (50 U.S.C. 1805(a)) is amended—

1 (1) in paragraph (3), by striking “; and” and
2 inserting a semicolon;

3 (2) in paragraph (4), by striking the period and
4 inserting “; and”; and

5 (3) by adding at the end the following:

6 “(5) for an application that is based, in any
7 part, on information obtained from the content of a
8 media source, on information gathered by a political
9 campaign, or on information relating to activity pro-
10 tected under the First Amendment to the Constitu-
11 tion of the United States—

12 “(A) such information is disclosed in the
13 application as having been so obtained or gath-
14 ered, or as being so related;

15 “(B) with regard to information gathered
16 from the content of a media source, the applica-
17 tion includes an explanation of the investigative
18 techniques used to corroborate the information;
19 and

20 “(C) with regard to information gathered
21 by a political campaign, such information is not
22 the sole source of the information used to jus-
23 tify the applicant’s belief described in section
24 104(a)(3).”.

1 (e) CONFORMING REPEAL OF RISAA EXCULPATORY
 2 INFORMATION REQUIREMENTS.—The Foreign Intel-
 3 ligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.)
 4 is amended—

5 (1) in section 104(a) (50 U.S.C. 1804(a)), by
 6 striking paragraph (13);

7 (2) in section 303(a) (50 U.S.C. 1823(a)), by
 8 striking paragraph (11);

9 (3) in section 402(c) (50 U.S.C. 1842(c))—

10 (A) in paragraph (3), by adding “and” at
 11 the end;

12 (B) in paragraph (4)(B), by striking “;
 13 and” and inserting a period; and

14 (C) by striking paragraph (5);

15 (4) in section 502(b)(2) (50 U.S.C.
 16 1862(b)(2))—

17 (A) in subparagraph (B), by adding “and”
 18 at the end;

19 (B) by redesignating subparagraph (E) as
 20 subparagraph (C);

21 (C) in subparagraph (C)(ii), as so redesign-
 22 nated, by striking “; and” and inserting a pe-
 23 riod; and

24 (D) by striking subparagraph (F);

1 (5) in section 703(b)(1) (50 U.S.C.
2 1881b(b)(1))—

3 (A) in subparagraph (J), by adding “and”
4 at the end;

5 (B) in subparagraph (K)(ii), by striking “;
6 and” and inserting a period; and

7 (C) by striking subparagraph (L); and

8 (6) in section 704(b) (50 U.S.C. 1881c(b))—

9 (A) in paragraph (7), by adding “and” at
10 the end;

11 (B) in paragraph (8)(B), by striking “;
12 and” and inserting a period; and

13 (C) by striking paragraph (9).

14 **SEC. 202. CRIMINAL PENALTIES FOR VIOLATIONS OF FISA.**

15 (a) IN GENERAL.—Section 109(a) of the Foreign In-
16 telligence Surveillance Act of 1978 (50 U.S.C. 1809(a))
17 is amended—

18 (1) in paragraph (2), by striking “or” at the
19 end;

20 (2) in paragraph (3), by striking the period at
21 the end and inserting a semicolon; and

22 (3) by adding at the end the following:

23 “(4) knowingly submits any document to or
24 makes any statement before the court established
25 under section 103(a) or the court established under

1 section 103(b), knowing such document or statement
2 to contain—

3 “(A) a false material declaration; or

4 “(B) a material omission; or

5 “(5) knowingly discloses the existence of an ap-
6 plication for an order authorizing surveillance under
7 this title, or any information contained therein, to
8 any person not authorized to receive such informa-
9 tion, except insofar as such disclosure is authorized
10 by statute or executive order setting forth permis-
11 sible disclosures by whistleblowers.”.

12 (b) **RULE OF CONSTRUCTION.**—This section and the
13 amendments made by this section may not be construed
14 to interfere with the enforcement of section 798 of title
15 18, United States Code, or any other provision of law re-
16 garding the unlawful disclosure of classified information.

17 **SEC. 203. AGENCY PROCEDURES TO ENSURE COMPLIANCE.**

18 (a) **AGENCY PROCEDURES TO ENSURE COMPLI-**
19 **ANCE.**—Title VI of the Foreign Intelligence Surveillance
20 Act of 1978 (50 U.S.C. 1871 et seq.) is amended by add-
21 ing at the end the following:

1 **“SEC. 605. AGENCY PROCEDURES TO ENSURE COMPLI-**
2 **ANCE.**

3 “The head of each Federal department or agency au-
4 thorized to acquire foreign intelligence information under
5 this Act shall establish procedures—

6 “(1) setting forth clear rules on what con-
7 stitutes a violation of this Act by an officer or em-
8 ployee of that department or agency; and

9 “(2) for taking appropriate adverse personnel
10 action against any officer or employee of the depart-
11 ment or agency who engages in a violation described
12 in paragraph (1), including more severe adverse per-
13 sonnel actions for any subsequent violation by such
14 officer or employee.”.

15 (b) CLERICAL AMENDMENT.—The table of contents
16 for the Foreign Intelligence Surveillance Act of 1978 is
17 amended by inserting after the item relating to section
18 604 the following:

 “Sec. 605. Agency procedures to ensure compliance.”.

19 (c) REPORT.—Not later than 90 days after the date
20 of enactment of this Act, the head of each Federal depart-
21 ment or agency that is required to establish procedures
22 under section 605 of the Foreign Intelligence Surveillance
23 Act of 1978, as added by subsection (a) of this section,
24 shall report to Congress on the implementation of such
25 procedures.

1 **SEC. 204. LIMIT ON CIVIL IMMUNITY FOR PROVIDING IN-**
2 **FORMATION, FACILITIES, OR TECHNICAL AS-**
3 **SISTANCE TO THE GOVERNMENT ABSENT A**
4 **COURT ORDER.**

5 Section 2511(2)(a) of title 18, United States Code,
6 is amended—

7 (1) in subparagraph (ii), by striking clause (B)
8 and inserting the following:

9 “(B) a certification in writing—

10 “(I) by a person specified in section
11 2518(7) or the Attorney General of the
12 United States;

13 “(II) that the requirements for an
14 emergency authorization to intercept a
15 wire, oral, or electronic communication
16 under section 2518(7) have been met; and

17 “(III) that the specified assistance is
18 required,”; and

19 (2) by striking subparagraph (iii) and inserting
20 the following:

21 “(iii) For assistance provided pursuant to a cer-
22 tification under subparagraph (ii)(B), the limitation
23 on causes of action under the last sentence of the
24 matter following that subparagraph shall only apply
25 to the extent that the assistance ceased at the ear-
26 liest of the time the application for a court order

1 was denied, the time the communication sought was
2 obtained, or 48 hours after the interception began.”.

3 **SEC. 205. PROHIBITION ON AVOIDING DISCLOSURE OBLI-**
4 **GATIONS THROUGH PARALLEL CONSTRUC-**
5 **TION.**

6 (a) DERIVED DEFINED.—

7 (1) IN GENERAL.—Section 101 of the Foreign
8 Intelligence Surveillance Act of 1978 (50 U.S.C.
9 1801) is amended by adding at the end the fol-
10 lowing:

11 “(q) ‘Derived from’, with respect to an electronic sur-
12 veillance, physical search, use of a pen register or trap
13 and trace device, production of tangible things, or acquisi-
14 tion under this Act or pursuant to executive authority,
15 means the Government would not have originally pos-
16 sessed the information or evidence but for that electronic
17 surveillance, physical search, use of a pen register or trap
18 and trace device, production of tangible things, or acquisi-
19 tion, which shall be determined without regard to any
20 claim that the information or evidence is attenuated from
21 the surveillance, search, use, production, or acquisition,
22 would inevitably have been discovered, or was subsequently
23 reobtained through other means.”.

(2) CONFORMING ADDITION TO OTHER TITLES.—The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended—

(A) in section 301(1) (50 U.S.C. 1821(1)), by inserting “‘derived from,’” after “‘destruction’,”;

(B) in section 401(1) (50 U.S.C. 1841(1)), by inserting “‘derived from,’” after “‘person’,”;

(C) in section 501(1) (50 U.S.C. 1861(1)), by inserting “‘derived from,’” after “‘terrorism’,”; and

(D) in section 701(a) (50 U.S.C. 1881(a)), by inserting “‘derived from,’” after “‘United States’,”.

(b) POLICIES AND GUIDANCE.—

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

(A) policies concerning the application of subsection (q) of section 101 of the Foreign Intelligence Surveillance Act of 1978, as added by subsection (a); and

(B) guidance for all members of the intelligence community (as defined in section 3 of

1 the National Security Act of 1947 (50 U.S.C.
2 3003)) and all Federal agencies with law en-
3 forcement responsibilities concerning the appli-
4 cation of subsection (q) of section 101 of the
5 Foreign Intelligence Surveillance Act of 1978,
6 as added by subsection (a).

7 (2) MODIFICATIONS.—Whenever the Attorney
8 General and the Director of National Intelligence
9 modify a policy or guidance published under para-
10 graph (1), the Attorney General and the Director
11 shall publish the modifications.

12 (c) USE OF INFORMATION ACQUIRED UNDER TITLE
13 VII.—Section 706 of the Foreign Intelligence Surveillance
14 Act of 1978 (50 U.S.C. 1881e) is amended—

15 (1) in subsection (a)(1), by striking “, except
16 for the purposes of subsection (j) of such section”;
17 and

18 (2) by amending subsection (b) to read as fol-
19 lows:

20 “(b) INFORMATION ACQUIRED UNDER SECTIONS
21 703, 704, OR 705.—Information acquired under section
22 703, 704, or 705 shall be deemed to be information ac-
23 quired from an electronic surveillance pursuant to title I
24 for the purposes of section 106.”.

1 **SEC. 206. SUNSET ON GRANDFATHER CLAUSE OF FISA'S**
 2 **BUSINESS RECORDS PROVISION.**

3 Section 102(b)(2) of the USA PATRIOT Improve-
 4 ment and Reauthorization Act of 2005 (Public Law 109–
 5 177; 50 U.S.C. 1805 note) is amended by inserting “, ex-
 6 cept that title V of the Foreign Intelligence Surveillance
 7 Act of 1978, as in effect on March 14, 2020, shall cease
 8 to be in effect with respect to such an investigation, of-
 9 fense, or potential offense on the date that is 180 days
 10 after the date of the enactment of the SAFE Act” after
 11 “continue in effect”.

12 **TITLE III—REFORMS RELATING**
 13 **TO PROCEEDINGS BEFORE**
 14 **THE FOREIGN INTELLIGENCE**
 15 **SURVEILLANCE COURT AND**
 16 **OTHER COURTS**

17 **SEC. 301. FOREIGN INTELLIGENCE SURVEILLANCE COURT**
 18 **REFORM.**

19 (a) EXPANSION OF APPOINTMENT AUTHORITY.—

20 (1) IN GENERAL.—Section 103(i)(2) of the For-
 21 eign Intelligence Surveillance Act of 1978 (50
 22 U.S.C. 1803(i)(2)) is amended—

23 (A) in subparagraph (A)—

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

1 “(i) shall, unless the court issues a
2 finding that appointment is not appro-
3 priate, appoint one or more individuals
4 who have been designated under paragraph
5 (1), not fewer than one of whom possesses
6 privacy and civil liberties expertise, unless
7 the court finds that such a qualification is
8 inappropriate, to serve as amicus curiae to
9 assist the court in the consideration of any
10 application or motion for an order or re-
11 view that, in the opinion of the court—

12 “(I) presents a novel or signifi-
13 cant interpretation of the law;

14 “(II) presents significant con-
15 cerns with respect to the activities of
16 a United States person that are pro-
17 tected by the first amendment to the
18 Constitution of the United States;

19 “(III) presents or involves a sen-
20 sitive investigative matter;

21 “(IV) presents a request for ap-
22 proval of a new program, a new tech-
23 nology, or a new use of existing tech-
24 nology;

1 “(V) presents a request for reau-
 2 thorization of programmatic surveil-
 3 lance; or

4 “(VI) otherwise presents novel or
 5 significant civil liberties issues;”; and

6 (ii) in clause (iii), by striking “, un-
 7 less the court issues a finding that such
 8 appointment is not appropriate or is likely
 9 to result in undue delay”;

10 (B) by striking subparagraph (B); and

11 (C) by redesignating subparagraph (C) as
 12 subparagraph (B).

13 (2) DEFINITION OF SENSITIVE INVESTIGATIVE
 14 MATTER.—Section 103(i) of the Foreign Intelligence
 15 Surveillance Act of 1978 (50 U.S.C. 1803(i)) is
 16 amended by adding at the end the following:

17 “(12) DEFINITION.—In this subsection, the
 18 term ‘sensitive investigative matter’ means—

19 “(A) an investigative matter involving the
 20 activities of—

21 “(i) a domestic public official or polit-
 22 ical candidate, or an individual serving on
 23 the staff of such an official or candidate;

24 “(ii) a domestic religious or political
 25 organization, or a known or suspected

1 United States person prominent in such an
 2 organization; or

3 “(iii) the domestic news media; or

4 “(B) any other investigative matter involv-
 5 ing a domestic entity or a known or suspected
 6 United States person that, in the judgment of
 7 the applicable court established under sub-
 8 section (a) or (b), is as sensitive as an inves-
 9 tigative matter described in subparagraph
 10 (A).”.

11 (b) AUTHORITY TO SEEK REVIEW.—Section 103(i)
 12 of the Foreign Intelligence Surveillance Act of 1978 (50
 13 U.S.C. 1803(i)), as amended by subsection (a) of this sec-
 14 tion, is amended—

15 (1) in paragraph (4)—

16 (A) in the paragraph heading, by inserting
 17 “; AUTHORITY” after “DUTIES”;

18 (B) in the matter preceding subparagraph
 19 (A), by striking “shall”;

20 (C) by striking subparagraph (A);

21 (D) by redesignating subparagraph (B) as
 22 subparagraph (A);

23 (E) in subparagraph (A), as so redesign-
 24 nated—

1 (i) in the matter preceding clause (i),
2 by inserting “shall” before “provide”;

3 (ii) in clause (i), by inserting before
4 the semicolon at the end the following: “,
5 including legal arguments regarding any
6 privacy or civil liberties interest of any
7 United States person that would be signifi-
8 cantly impacted by the application or mo-
9 tion”; and

10 (iii) in clause (iii), by striking the pe-
11 riod at the end and inserting “; and”; and
12 (F) by adding at the end the following:

13 “(B) may seek leave to raise any novel or
14 significant privacy or civil liberties issue rel-
15 evant to the application or motion or other
16 issue directly impacting the legality of the pro-
17 posed electronic surveillance with the court, re-
18 gardless of whether the court has requested as-
19 sistance on that issue.”;

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

23 (3) by inserting after paragraph (6) the fol-
24 lowing:

1 “(7) AUTHORITY TO SEEK REVIEW OF DECI-
2 SIONS.—

3 “(A) FISA COURT DECISIONS.—

4 “(i) PETITION.—Following issuance of
5 an order under this Act by the court estab-
6 lished under subsection (a), an amicus cu-
7 riae appointed under paragraph (2) may
8 petition the court to certify for review to
9 the court established under subsection (b)
10 a question of law pursuant to subsection
11 (j).

12 “(ii) WRITTEN STATEMENT OF REA-
13 SONS.—If the court established under sub-
14 section (a) denies a petition under this
15 subparagraph, the court shall provide for
16 the record a written statement of the rea-
17 sons for the denial.

18 “(iii) APPOINTMENT.—Upon certifi-
19 cation of any question of law pursuant to
20 this subparagraph, the court established
21 under subsection (b) shall appoint the ami-
22 cus curiae to assist the court in its consid-
23 eration of the certified question, unless the
24 court issues a finding that such appoint-
25 ment is not appropriate.

“(B) FISA COURT OF REVIEW DECISIONS.—An amicus curiae appointed under paragraph (2) may petition the court established under subsection (b) 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 section 602(a).”.

(c) ACCESS TO INFORMATION.—

(1) APPLICATION AND MATERIALS.—Section 103(i)(6) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(i)(6)) is amended by striking subparagraph (A) and inserting the following:

“(A) IN GENERAL.—

“(i) RIGHT OF AMICUS.—If a court established under subsection (a) or (b) ap-

1 points an amicus curiae under paragraph
2 (2), the amicus curiae—

3 “(I) shall have access, to the ex-
4 tent such information is available to
5 the Government, to—

6 “(aa) the application, certifi-
7 cation, petition, motion, and
8 other information and supporting
9 materials, including any informa-
10 tion described in section 901,
11 submitted to the court estab-
12 lished under subsection (a) in
13 connection with the matter in
14 which the amicus curiae has been
15 appointed, including access to
16 any relevant legal precedent (in-
17 cluding any such precedent that
18 is cited by the Government, in-
19 cluding in such an application);

20 “(bb) an unredacted copy of
21 each relevant decision made by
22 the court established under sub-
23 section (a) or the court estab-
24 lished under subsection (b) in
25 which the court decides a ques-

1 tion of law, without regard to
 2 whether the decision is classified;
 3 and

4 “(cc) any other information
 5 or materials that the court deter-
 6 mines are relevant to the duties
 7 of the amicus curiae; and

8 “(II) may make a submission to
 9 the court requesting access to any
 10 other particular materials or informa-
 11 tion (or category of materials or infor-
 12 mation) that the amicus curiae be-
 13 lieves to be relevant to the duties of
 14 the amicus curiae.

15 “(ii) SUPPORTING DOCUMENTATION
 16 REGARDING ACCURACY.—The court estab-
 17 lished under subsection (a), upon the mo-
 18 tion of an amicus curiae appointed under
 19 paragraph (2) or upon its own motion,
 20 may require the Government to make
 21 available the supporting documentation de-
 22 scribed in section 902.”.

23 (2) CLARIFICATION OF ACCESS TO CERTAIN IN-
 24 FORMATION.—Section 103(i)(6) of the Foreign In-

1 telligence Surveillance Act of 1978 (50 U.S.C.
2 1803(i)(6)) is amended—

3 (A) in subparagraph (B), by striking
4 “may” and inserting “shall”; and

5 (B) by striking subparagraph (C) and in-
6 serting the following:

7 “(C) CLASSIFIED INFORMATION.—An ami-
8 cus curiae designated or appointed by the court
9 shall have access, to the extent such informa-
10 tion is available to the Government, to
11 unredacted copies of each opinion, order, tran-
12 script, pleading, or other document of the court
13 established under subsection (a) and the court
14 established under subsection (b), including, if
15 the individual is eligible for access to classified
16 information, any classified documents, informa-
17 tion, and other materials or proceedings.”.

18 (3) CONSULTATION AMONG AMICI CURIAE.—
19 Section 103(i)(6) of the Foreign Intelligence Surveil-
20 lance Act of 1978 (50 U.S.C. 1803(i)(6)) is amend-
21 ed—

22 (A) by redesignating subparagraph (D) as
23 subparagraph (E); and

24 (B) by inserting after subparagraph (C)
25 the following:

1 “(D) CONSULTATION AMONG AMICI CU-
 2 RIAE.—An amicus curiae appointed under para-
 3 graph (2) by the court established under sub-
 4 section (a) or the court established under sub-
 5 section (b) may consult with 1 or more of the
 6 other individuals designated by the court to
 7 serve as amicus curiae pursuant to paragraph
 8 (1) of this subsection regarding any of the in-
 9 formation relevant to any assigned pro-
 10 ceeding.”.

11 (d) EFFECTIVE DATE.—The amendments made by
 12 this section shall take effect on the date of enactment of
 13 this Act and shall apply with respect to proceedings under
 14 the Foreign Intelligence Surveillance Act of 1978 (50
 15 U.S.C. 1801 et seq.) that take place on or after, or are
 16 pending on, that date.

17 **SEC. 302. PUBLIC DISCLOSURE AND DECLASSIFICATION OF**
 18 **CERTAIN DOCUMENTS.**

19 Section 602(a) of the Foreign Intelligence Surveil-
 20 lance Act of 1978 (50 U.S.C. 1872(a)) is amended—

21 (1) by striking “, to be concluded as soon as
 22 practicable, but not later than 180 days after the
 23 commencement of such review,”; and

24 (2) by inserting “to be concluded as soon as
 25 practicable, but not later than 180 days after the

1 issuance of such decision, order, or opinion,” before
 2 “and, consistent with that review”.

3 **SEC. 303. TECHNICAL AMENDMENT TO CONTEMPT POWER**
 4 **OF FISC AND FISC-R.**

5 (a) IN GENERAL.—Chapter 21 of title 18, United
 6 States Code, is amended—

7 (1) in section 402, by striking “, including the
 8 Foreign Intelligence Surveillance Court or the For-
 9 eign Intelligence Surveillance Court of Review estab-
 10 lished by section 103 of the Foreign Intelligence
 11 Surveillance Act of 1978 (50 U.S.C. 1803),” and in-
 12 serting the following: “, the Foreign Intelligence
 13 Surveillance Court, the Foreign Intelligence Surveil-
 14 lance Court of Review,”; and

15 (2) by adding at the end the following:

16 **“§ 404. Definitions**

17 “For purposes of this chapter—

18 “(1) the term ‘court of the United States’ in-
 19 cludes the Foreign Intelligence Surveillance Court or
 20 the Foreign Intelligence Surveillance Court of Re-
 21 view; and

22 “(2) the terms ‘Foreign Intelligence Surveil-
 23 lance Court’ and ‘Foreign Intelligence Surveillance
 24 Court of Review’ have the meanings given those

1 terms in section 601(e) of the Foreign Intelligence
2 Surveillance Act of 1978 (50 U.S.C. 1871(e)).”.

3 (b) CLERICAL AMENDMENT.—The table of sections
4 for chapter 21 of title 18, United States Code, is amended
5 by adding at the end the following:

“404. Definitions.”.

6 **TITLE IV—INDEPENDENT EXEC-** 7 **UTIVE BRANCH OVERSIGHT**

8 **SEC. 401. PERIODIC AUDIT OF FISA COMPLIANCE BY IN-** 9 **SPECTOR GENERAL.**

10 (a) REPORT REQUIRED.—Title VI of the Foreign In-
11 telligence Surveillance Act of 1978 (50 U.S.C. 1871 et
12 seq.), as amended by section 203 of this Act, is amended
13 by adding at the end the following:

14 **“SEC. 606. PERIODIC AUDIT OF FISA COMPLIANCE BY IN-** 15 **SPECTOR GENERAL.**

16 “Not later than June 30 of the first calendar year
17 that begins after the date of enactment of this section,
18 and every 3 years thereafter, the Inspector General of the
19 Department of Justice shall—

20 “(1) conduct an audit of alleged or potential
21 violations and failures to comply with the require-
22 ments of this Act, and any procedures established
23 pursuant to this Act, which shall include an analysis
24 of the accuracy and completeness of applications and

1 certifications for orders submitted under each of sec-
 2 tions 105, 303, 402, 502, 702, 703, and 704; and

3 “(2) submit to the Select Committee on Intel-
 4 ligence of the Senate, the Committee on the Judici-
 5 ary of the Senate, the Permanent Select Committee
 6 on Intelligence of the House of Representatives, and
 7 the Committee on the Judiciary of the House of
 8 Representatives a report on the audit required under
 9 paragraph (1).”.

10 (b) CLERICAL AMENDMENT.—The table of contents
 11 for the Foreign Intelligence Surveillance Act of 1978, as
 12 amended by section 203 of this Act, is amended by insert-
 13 ing after the item relating to section 605 the following:

“Sec. 606. Periodic audit of FISA compliance by Inspector General.”.

14 **TITLE V—PROTECTIONS FOR**
 15 **UNITED STATES PERSONS**
 16 **WHOSE SENSITIVE INFORMA-**
 17 **TION IS PURCHASED BY IN-**
 18 **TELLIGENCE AND LAW EN-**
 19 **FORCEMENT AGENCIES**

20 **SEC. 501. LIMITATION ON INTELLIGENCE ACQUISITION OF**
 21 **UNITED STATES PERSON DATA.**

22 (a) DEFINITIONS.—In this section:

23 (1) APPROPRIATE COMMITTEES OF CON-
 24 GRESS.—The term “appropriate committees of Con-
 25 gress” means—

1 (A) the congressional intelligence commit-
2 tees (as defined in section 3 of the National Se-
3 curity Act of 1947 (50 U.S.C. 3003));

4 (B) the Committee on the Judiciary of the
5 Senate; and

6 (C) the Committee on the Judiciary of the
7 House of Representatives.

8 (2) COVERED DATA.—The term “covered data”
9 means data, derived data, or any unique identifier
10 that—

11 (A) is linked to or is reasonably linkable to
12 a covered person; and

13 (B) does not include—

14 (i) data that—

15 (I) is lawfully available to the
16 public through Federal, State, or local
17 government records or through widely
18 distributed media;

19 (II) is reasonably believed to have
20 been voluntarily made available to the
21 general public by the covered person;
22 or

23 (III) is a specific communication
24 or transaction with a targeted indi-
25 vidual who is not a covered person; or

1 (ii) human intelligence other than
2 data transfers.

3 (3) COVERED PERSON.—The term “covered
4 person” means an individual who—

5 (A) is reasonably believed to be located in
6 the United States at the time of the creation or
7 acquisition of the covered data; or

8 (B) is a United States person.

9 (4) INTELLIGENCE COMMUNITY.—The term
10 “intelligence community” has the meaning given
11 such term in section 3 of the National Security Act
12 of 1947 (50 U.S.C. 3003).

13 (5) STATE, UNITED STATES, UNITED STATES
14 PERSON.—The terms “State”, “United States”, and
15 “United States person” have the meanings given
16 such terms in section 101 of the Foreign Intelligence
17 Surveillance Act of 1978 (50 U.S.C. 1801).

18 (b) LIMITATION.—

19 (1) IN GENERAL.—Subject to paragraphs (2)
20 through (7), an element of the intelligence commu-
21 nity may not acquire covered data, which shall in-
22 clude acquiring covered data directly or indirectly,
23 such as by acquiring covered data from another enti-
24 ty that directly acquired the covered data.

1 (2) AUTHORIZATION PURSUANT TO COURT
 2 ORDER.—An element of the intelligence community
 3 may acquire covered data if the collection has been
 4 authorized by an order issued pursuant to the For-
 5 eign Intelligence Surveillance Act of 1978 (50
 6 U.S.C. 1801 et seq.) or title 18, United States Code,
 7 by a court of competent jurisdiction covering the pe-
 8 riod of the acquisition, subject to the use, dissemina-
 9 tion, querying, retention, and other minimization
 10 limitations required by such authorization.

11 (3) AUTHORIZATION FOR EMPLOYMENT-RE-
 12 LATED USE.—An element of the intelligence commu-
 13 nity may acquire covered data about an employee of,
 14 or applicant for employment by, an element of the
 15 intelligence community for employment-related pur-
 16 poses, but only if—

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

19 (B) the covered data is destroyed at such
 20 time as it is no longer necessary for such pur-
 21 poses.

22 (4) EXCEPTION FOR COMPLIANCE PURPOSES.—
 23 An element of the intelligence community may ac-
 24 quire covered data for the purpose of supporting
 25 compliance with collection limitations and minimiza-

tion requirements imposed by statute, guidelines, procedures, or the Constitution of the United States, but only if—

(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 there is a reasonable belief that an emergency exists involving an imminent threat of death or serious bodily harm and the covered data is necessary to mitigate that threat, but only if—

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

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

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

(A) each covered person linked or reasonably linkable to the covered data, or, if such person is incapable of providing consent, a third

1 party legally authorized to consent on behalf of
2 the person, has provided consent to the acquisi-
3 tion and use of the data on a case-by-case
4 basis;

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

8 (C) the covered data is destroyed at such
9 time as it is no longer necessary for such pur-
10 poses.

11 (7) EXCEPTION FOR NONSEGREGABLE DATA.—

12 An element of the intelligence community may ac-
13 quire a dataset that includes covered data if the cov-
14 ered data is not reasonably segregable prior to ac-
15 quisition, but only if the element of the intelligence
16 community complies with the minimization proce-
17 dures in subsection (c).

18 (c) MINIMIZATION PROCEDURES.—

19 (1) IN GENERAL.—The Attorney General shall
20 adopt specific procedures that are reasonably de-
21 signed to minimize the acquisition and retention,
22 and to restrict the querying, of covered data that is
23 not subject to 1 or more of the exceptions set forth
24 in subsection (b).

1 (2) ACQUISITION AND RETENTION.—The proce-
2 dures adopted under paragraph (1) shall require ele-
3 ments of the intelligence community to exhaust all
4 reasonable means—

5 (A) to exclude covered data not subject to
6 1 or more exceptions set forth in subsection (b)
7 from datasets prior to acquisition; and

8 (B) to remove and delete covered data not
9 subject to 1 or more exceptions set forth in sub-
10 section (b) prior to the operational use of the
11 acquired dataset or the inclusion of the dataset
12 in a database intended for operational use.

13 (3) DESTRUCTION.—The procedures adopted
14 under paragraph (1) shall require that if an element
15 of the intelligence community identifies covered data
16 not subject to 1 or more exceptions set forth in
17 paragraphs (2) through (6) of subsection (b), such
18 covered data shall be promptly destroyed.

19 (4) QUERYING.—

20 (A) IN GENERAL.—Except as provided in
21 subparagraphs (B) and (C), no officer or em-
22 ployee of an element of the intelligence commu-
23 nity may conduct a query of covered data, in-
24 cluding covered data already subjected to mini-

1 mization, in an effort to find records of or
2 about a particular covered person.

3 (B) EXCEPTIONS.—Subparagraph (A)
4 shall not apply to a query related to a par-
5 ticular covered person if—

6 (i) such covered person is the subject
7 of a court order issued under the Foreign
8 Intelligence Surveillance Act of 1978 (50
9 U.S.C. 1801 et seq.) or title 18, United
10 States Code, that would authorize the ele-
11 ment of the intelligence community to com-
12 pel the production of the covered data,
13 during the effective period of that order;

14 (ii) the purpose of the query is to re-
15 trieve information about an employee of, or
16 applicant for employment by, an element of
17 the intelligence community, provided that
18 any covered data accessed through such
19 query is used only for such purpose;

20 (iii) the query is conducted for the
21 purpose of supporting compliance with col-
22 lection limitations and minimization re-
23 quirements imposed by statute, guidelines,
24 procedures, or the Constitution of the
25 United States, provided that any covered

1 data accessed through such query is used
2 only for such purpose;

3 (iv) the officer or employee of an ele-
4 ment of the intelligence community car-
5 rying out the query has a reasonable belief
6 that an emergency exists involving an im-
7 minent threat of death or serious bodily
8 harm, and that in order to prevent or miti-
9 gate such threat, the query must be con-
10 ducted before a court order can, with due
11 diligence, be obtained, provided that any
12 covered data accessed through such query
13 is used only for such purpose; or

14 (v) such covered person or, if such
15 person is incapable of providing consent, a
16 third party legally authorized to consent on
17 behalf of the person has consented to the
18 query, provided that any use of covered
19 data accessed through such query is lim-
20 ited to the purposes for which the consent
21 was provided.

22 (C) SPECIAL RULE FOR NONSEGREGABLE
23 DATASETS.—For a query of a dataset acquired
24 under subsection (b)(7)—

1 (i) each query shall be reasonably de-
2 signed to exclude personal data of covered
3 persons, unless the query is subject to an
4 exception set forth in subparagraph (B);
5 and

6 (ii) any personal data of covered per-
7 sons returned pursuant to a query that is
8 not subject to an exception set forth in
9 paragraphs (2) through (7) of subsection
10 (b) shall not be reviewed and shall imme-
11 diately be destroyed.

12 (d) PROHIBITION ON USE OF DATA OBTAINED IN
13 VIOLATION OF THIS SECTION.—Covered data acquired by
14 an element of the intelligence community in violation of
15 subsection (b), and any evidence derived therefrom, may
16 not be used, received in evidence, or otherwise dissemi-
17 nated in any investigation by or in any trial, hearing, or
18 other proceeding in or before any court, grand jury, de-
19 partment, office, agency, regulatory body, legislative com-
20 mittee, or other authority of the United States, a State,
21 or political subdivision thereof.

22 (e) REPORTING REQUIREMENT.—

23 (1) IN GENERAL.—Not later than 180 days
24 after the date of the enactment of this Act, the Di-
25 rector of National Intelligence shall submit to the

1 appropriate committees of Congress and the Privacy
2 and Civil Liberties Oversight Board a report on the
3 acquisition of datasets that the Director anticipates
4 will contain information of covered persons that is
5 significant in volume, proportion, or sensitivity.

6 (2) CONTENTS.—The report submitted pursu-
7 ant to paragraph (1) shall include the following:

8 (A) A description of the covered person in-
9 formation in each dataset.

10 (B) An estimate of the amount of covered
11 person information in each dataset.

12 (3) NOTIFICATIONS.—After submitting the re-
13 port required by paragraph (1), the Director shall,
14 in coordination with the Under Secretary of Defense
15 for Intelligence and Security, notify the appropriate
16 committees of Congress of any changes to the infor-
17 mation contained in such report.

18 (4) AVAILABILITY TO THE PUBLIC.—The Direc-
19 tor shall make available to the public on the website
20 of the Director—

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

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

1 (f) RULE OF CONSTRUCTION.—Nothing in this sec-
 2 tion shall authorize an acquisition otherwise prohibited by
 3 the Foreign Intelligence Surveillance Act of 1978 (50
 4 U.S.C. 1801 et seq.) or title 18, United States Code.

5 **SEC. 502. LIMITATION ON LAW ENFORCEMENT PURCHASE**
 6 **OF PERSONAL DATA FROM DATA BROKERS.**

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

9 “(e) PROHIBITION ON OBTAINING IN EXCHANGE FOR
 10 ANYTHING OF VALUE PERSONAL DATA BY LAW EN-
 11 FORCEMENT AGENCIES.—

12 “(1) DEFINITIONS.—In this subsection and
 13 subsection (f)—

14 “(A) the term ‘covered governmental enti-
 15 ty’ means a law enforcement agency of a gov-
 16 ernmental entity;

17 “(B) the term ‘covered organization’
 18 means a person who—

19 “(i) is not a governmental entity; and

20 “(ii) is not an individual;

21 “(C) the term ‘covered person’ means an
 22 individual who—

23 “(i) is reasonably believed to be lo-
 24 cated inside the United States at the time

1 of the creation of the covered personal
2 data; or

3 “(ii) is a United States person, as de-
4 fined in section 101 of the Foreign Intel-
5 ligence Surveillance Act of 1978 (50
6 U.S.C. 1801);

7 “(D) the term ‘covered personal data’
8 means personal data relating to a covered per-
9 son;

10 “(E) the term ‘electronic device’ has the
11 meaning given the term ‘computer’ in section
12 1030(e);

13 “(F) the term ‘lawfully obtained public
14 data’ means personal data obtained by a par-
15 ticular covered organization that the covered or-
16 ganization—

17 “(i) reasonably understood to have
18 been voluntarily made available to the gen-
19 eral public by the covered person; and

20 “(ii) obtained in compliance with all
21 applicable laws, regulations, contracts, pri-
22 vacy policies, and terms of service;

23 “(G) the term ‘obtain in exchange for any-
24 thing of value’ means to obtain by purchasing,
25 to receive in connection with services being pro-

1 vided for monetary or nonmonetary consider-
2 ation, or to otherwise obtain in exchange for
3 consideration, including an access fee, service
4 fee, maintenance fee, or licensing fee; and

5 “(H) the term ‘personal data’—

6 “(i) means data, derived data, or any
7 unique identifier that is linked to, or is
8 reasonably linkable to, an individual or to
9 an electronic device that is linked to, or is
10 reasonably linkable to, 1 or more individ-
11 uals in a household;

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

18 “(iii) does not include—

19 “(I) data that is lawfully avail-
20 able through Federal, State, or local
21 government records or through widely
22 distributed media; or

23 “(II) a specific communication or
24 transaction with a targeted individual
25 who is not a covered person.

1 “(2) LIMITATION.—

2 “(A) IN GENERAL.—

3 “(i) PROHIBITION.—Subject to
4 clauses (ii) through (x), a covered govern-
5 mental entity may not obtain in exchange
6 for anything of value covered personal data
7 if—

8 “(I) the covered personal data is
9 directly or indirectly obtained from a
10 covered organization; or

11 “(II) the covered personal data is
12 derived from covered personal data
13 that was directly or indirectly ob-
14 tained from a covered organization.

15 “(ii) EXCEPTION FOR CERTAIN COM-
16 PILATIONS OF DATA.—A covered govern-
17 mental entity may obtain in exchange for
18 something of value covered personal data
19 as part of a larger compilation of data
20 which includes personal data about persons
21 who are not covered persons, if—

22 “(I) the covered governmental
23 entity is unable through reasonable
24 means to exclude covered personal

1 data from the larger compilation ob-
2 tained; and

3 “(II) the covered governmental
4 entity minimizes any covered personal
5 data from the larger compilation, in
6 accordance with subsection (f).

7 “(iii) EXCEPTION FOR WHISTLE-
8 BLOWER DISCLOSURES TO LAW ENFORCE-
9 MENT.—Clause (i) shall not apply to cov-
10 ered personal data that is obtained by a
11 covered governmental entity under a pro-
12 gram established by an Act of Congress
13 under which a portion of a penalty or a
14 similar payment or bounty is paid to an in-
15 dividual who discloses information about
16 an unlawful activity to the Government,
17 such as the program authorized under sec-
18 tion 7623 of the Internal Revenue Code of
19 1986 (relating to awards to whistleblowers
20 in cases of underpayments or fraud).

21 “(iv) EXCEPTION FOR COST REIM-
22 BURSEMENT UNDER COMPULSORY LEGAL
23 PROCESS.—Clause (i) shall not apply to
24 covered personal data that is obtained by

1 a covered governmental entity from a cov-
2 ered organization in accordance with com-
3 pulsory legal process that—

4 “(I) is established by a Federal
5 or State statute; and

6 “(II) provides for the reimburse-
7 ment of costs of the covered organiza-
8 tion that are incurred in connection
9 with providing the record or informa-
10 tion to the covered governmental enti-
11 ty, such as the reimbursement of costs
12 under section 2706.

13 “(v) EXCEPTION FOR EMPLOYMENT-
14 RELATED USE.—Clause (i) shall not apply
15 to covered personal data about an em-
16 ployee of, or applicant for employment by,
17 a covered governmental entity that is—

18 “(I) obtained by the covered gov-
19 ernmental entity for employment-re-
20 lated purposes;

21 “(II) accessed and used by the
22 covered governmental entity only for
23 employment-related purposes; and

24 “(III) destroyed at such time as
25 the covered personal data is no longer

1 needed for employment-related pur-
2 poses.

3 “(vi) EXCEPTION FOR USE IN BACK-
4 GROUND CHECKS.—Clause (i) shall not
5 apply to covered personal data about a cov-
6 ered person that is—

7 “(I) obtained by a covered gov-
8 ernmental entity for purposes of con-
9 ducting a background check of the
10 covered person with the written con-
11 sent of the covered person;

12 “(II) accessed and used by the
13 covered governmental entity only for
14 background check-related purposes;
15 and

16 “(III) destroyed at such time as
17 the covered personal data is no longer
18 needed for background check-related
19 purposes.

20 “(vii) EXCEPTION FOR LAWFULLY OB-
21 TAINED PUBLIC DATA.—Clause (i) shall
22 not apply to covered personal data that is
23 obtained by a covered governmental entity
24 if—

1 “(I) the covered personal data is
2 lawfully obtained public data; or

3 “(II) the covered personal data is
4 derived from covered personal data
5 that solely consists of lawfully ob-
6 tained public data.

7 “(viii) EXCEPTION FOR LIFE OR
8 SAFETY.—Clause (i) shall not apply to cov-
9 ered personal data that is obtained by a
10 covered governmental entity if there is a
11 reasonable belief than an emergency exists
12 involving an imminent threat of death or
13 serious bodily harm to a covered person
14 and the covered data is necessary to miti-
15 gate that threat, provided that—

16 “(I) access to and use of the cov-
17 ered personal data is limited to ad-
18 dressing the threat; and

19 “(II) the covered personal data is
20 destroyed at such time as it is no
21 longer necessary for such purpose.

22 “(ix) EXCEPTION FOR COMPLIANCE
23 PURPOSES.—Clause (i) shall not apply to
24 covered personal data that is obtained by
25 a covered governmental entity for the pur-

pose of supporting compliance with collection limitations and minimization requirements imposed by statute, guidelines, procedures, or the Constitution of the United States, provided that—

“(I) access to and use of the covered personal data is limited to such purpose; and

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

“(x) EXCEPTION FOR CONSENT.— Clause (i) shall not apply to covered personal data that is obtained by a covered governmental entity if—

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

1 “(II) access to and use of the
2 covered personal data is limited to the
3 purposes for which the consent was
4 provided; and

5 “(III) the covered personal data
6 is destroyed at such time as it is no
7 longer necessary for such purposes.

8 “(B) INDIRECTLY ACQUIRED RECORDS
9 AND INFORMATION.—The limitation under sub-
10 paragraph (A) shall apply without regard to
11 whether the covered organization possessing the
12 covered personal data is the covered organiza-
13 tion that initially obtained or collected, or is the
14 covered organization that initially received the
15 disclosure of, the covered personal data.

16 “(3) LIMIT ON SHARING BETWEEN AGEN-
17 CIES.—An agency of a governmental entity that is
18 not a covered governmental entity may not provide
19 to a covered governmental entity covered personal
20 data that was obtained in a manner that would vio-
21 late paragraph (2) if the agency of a governmental
22 entity were a covered governmental entity, unless the
23 covered governmental entity would have been per-
24 mitted to obtain the covered personal data under an
25 exception set forth in paragraph (2)(A).

1 “(4) PROHIBITION ON USE OF DATA OBTAINED
2 IN VIOLATION OF THIS SECTION.—

3 “(A) IN GENERAL.—Covered personal data
4 obtained by or provided to a covered govern-
5 mental entity in violation of paragraph (2) or
6 (3), and any evidence derived therefrom, may
7 not be used, received in evidence, or otherwise
8 disseminated by, on behalf of, or upon a motion
9 or other action by a covered governmental enti-
10 ty in any investigation by or in any trial, hear-
11 ing, or other proceeding in or before any court,
12 grand jury, department, officer, agency, regu-
13 latory body, legislative committee, or other au-
14 thority of the United States, a State, or a polit-
15 ical subdivision thereof.

16 “(B) USE BY AGGRIEVED PARTIES.—Noth-
17 ing in subparagraph (A) shall be construed to
18 limit the use of covered personal data by a cov-
19 ered person aggrieved of a violation of para-
20 graph (2) or (3) in connection with any action
21 relating to such a violation.

22 “(f) MINIMIZATION PROCEDURES.—

23 “(1) IN GENERAL.—The Attorney General shall
24 adopt specific procedures that are reasonably de-
25 signed to minimize the acquisition and retention,

1 and to restrict the querying, of covered personal
2 data, and prohibit the dissemination of information
3 derived from covered personal data.

4 “(2) ACQUISITION AND RETENTION.—The pro-
5 cedures adopted under paragraph (1) shall require
6 covered governmental entities to exhaust all reason-
7 able means—

8 “(A) to exclude covered personal data that
9 is not subject to 1 or more of the exceptions set
10 forth in clauses (iii) through (x) of subsection
11 (e)(2)(A) from the data obtained; and

12 “(B) to remove and delete covered personal
13 data described in subparagraph (A) not subject
14 to 1 or more exceptions set forth in clauses (iii)
15 through (x) of subsection (e)(2)(A) after a com-
16 pilation is obtained and before operational use
17 of the compilation or inclusion of the compila-
18 tion in a dataset intended for operational use.

19 “(3) DESTRUCTION.—The procedures adopted
20 under paragraph (1) shall require that, if a covered
21 governmental entity identifies covered personal data
22 in a compilation described in clause (ii) of subsection
23 (e)(2)(A) not subject to 1 or more exceptions set
24 forth in clauses (iii) through (x) of such subsection,
25 the covered governmental entity shall promptly de-

1 stroy the covered personal data and any dissemina-
2 tion of information derived from the covered per-
3 sonal data shall be prohibited.

4 “(4) QUERYING.—

5 “(A) IN GENERAL.—Except as provided in
6 subparagraphs (B) and (C), no officer or em-
7 ployee of a covered governmental entity may
8 conduct a query of personal data, including per-
9 sonal data already subjected to minimization, in
10 an effort to find records of or about a par-
11 ticular covered person.

12 “(B) EXCEPTIONS.—Subparagraph (A)
13 shall not apply to a query related to a par-
14 ticular covered person if—

15 “(i) such covered person is the subject
16 of a court order issued under this title that
17 would authorize the covered governmental
18 entity to compel the production of the cov-
19 ered personal data, during the effective pe-
20 riod of that order;

21 “(ii) the purpose of the query is to re-
22 trieve information obtained by a covered
23 governmental entity under a program es-
24 tablished by an Act of Congress under
25 which a portion of a penalty or a similar

1 payment or bounty is paid to an individual
2 who discloses information about an unlaw-
3 ful activity to the Government, such as the
4 program authorized under section 7623 of
5 the Internal Revenue Code of 1986 (relat-
6 ing to awards to whistleblowers in cases of
7 underpayments or fraud), provided that
8 any covered personal data accessed
9 through such query is used only for such
10 purpose;

11 “(iii) the purpose of the query is to
12 retrieve information about an employee of,
13 or applicant for employment by, a covered
14 governmental entity that has been obtained
15 by the covered governmental entity for em-
16 ployment-related purposes, provided that
17 any covered personal data accessed
18 through such query is used only for such
19 purposes;

20 “(iv) the purpose of the query is to re-
21 trieve information obtained by a covered
22 governmental entity for purposes of con-
23 ducting a background check of the covered
24 person with the written consent of the cov-
25 ered person, provided that any covered per-

1 sonal data accessed through such query is
2 used only for such purposes;

3 “(v) the purpose of the query is to re-
4 trieve, and the query is reasonably de-
5 signed to retrieve, only lawfully obtained
6 public data, and only lawfully obtained
7 public data is accessed and used as a re-
8 sult of the query;

9 “(vi) the officer or employee of a cov-
10 ered governmental entity carrying out the
11 query has a reasonable belief that an emer-
12 gency exists involving an imminent threat
13 of death or serious bodily harm, and in
14 order to prevent or mitigate that threat,
15 the query must be conducted before a
16 court order can, with due diligence, be ob-
17 tained, provided that any covered personal
18 data accessed through such query is used
19 only for such purpose;

20 “(vii) the query is conducted for the
21 purpose of supporting compliance with col-
22 lection limitations and minimization re-
23 quirements imposed by statute, guidelines,
24 procedures, or the Constitution of the
25 United States, provided that any covered

1 personal data accessed through such query
2 is used only for such purpose; or

3 “(viii) such covered person or, if such
4 covered person is incapable of providing
5 consent, a third party legally authorized to
6 consent on behalf of the covered person
7 has consented to the query, provided that
8 any use of covered personal data accessed
9 through such query is limited to the pur-
10 poses for which the consent was provided.

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

14 “(i) each query shall be reasonably de-
15 signed to exclude personal data of covered
16 persons, unless the query is subject to an
17 exception set forth in subparagraph (B);
18 and

19 “(ii) any personal data of covered per-
20 sons returned pursuant to a query that is
21 not subject to an exception set forth in
22 clauses (ii) through (x) of subsection
23 (e)(2)(A) shall not be reviewed and shall
24 immediately be destroyed.”.

1 **SEC. 503. CONSISTENT PROTECTIONS FOR DEMANDS FOR**
2 **DATA HELD BY INTERACTIVE COMPUTING**
3 **SERVICES.**

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

6 (1) in paragraph (3)(C), by striking “and” at
7 the end;

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

10 (3) by adding at the end the following:

11 “(5) the term ‘online service provider’ means a
12 provider of electronic communication service, a pro-
13 vider of remote computing service, any information
14 service, system, or access software provider that pro-
15 vides or enables computer access by multiple users
16 to a computer server, including specifically a service
17 or system that provides access to the Internet and
18 such systems operated or services offered by libraries
19 or educational institutions; and”.

20 (b) REQUIRED DISCLOSURE.—Section 2703 of title
21 18, United States Code, is amended—

22 (1) in subsection (a), in the first sentence, by
23 striking “a provider of electronic communication
24 service” and inserting “an online service provider”;

25 (2) in subsection (c)—

1 (A) in paragraph (1), in the matter pre-
2 ceding subparagraph (A), by striking “a pro-
3 vider of electronic communication service or re-
4 mote computing service” and inserting “an on-
5 line service provider”; and

6 (B) in paragraph (2), in the matter pre-
7 ceding subparagraph (A), by striking “A pro-
8 vider of electronic communication service or re-
9 mote computing service” and inserting “An on-
10 line service provider”; and

11 (3) in subsection (g), by striking “a provider of
12 electronic communications service or remote com-
13 puting service” and inserting “an online service pro-
14 vider”.

15 (c) LIMITATION ON VOLUNTARY DISCLOSURE.—Sec-
16 tion 2702(a) of title 18, United States Code, is amended—

17 (1) in paragraph (1), by striking “a person or
18 entity providing an electronic communication service
19 to the public” and inserting “an online service pro-
20 vider”;

21 (2) in paragraph (2), by striking “a person or
22 entity providing remote computing service to the
23 public” and inserting “an online service provider”;
24 and

1 (3) in paragraph (3), by striking “a provider of
 2 remote computing service or electronic communica-
 3 tion service to the public” and inserting “an online
 4 service provider”.

5 **SEC. 504. CONSISTENT PRIVACY PROTECTIONS FOR DATA**
 6 **HELD BY DATA BROKERS.**

7 Section 2703 of title 18, United States Code is
 8 amended by adding at the end the following:

9 “(i) COVERED PERSONAL DATA.—

10 “(1) DEFINITIONS.—In this subsection, the
 11 terms ‘covered personal data’ and ‘covered organiza-
 12 tion’ have the meanings given such terms in section
 13 2702(e).

14 “(2) LIMITATION.—Unless a governmental enti-
 15 ty obtains an order in accordance with paragraph
 16 (3), the governmental entity may not require a cov-
 17 ered organization that is not an online service pro-
 18 vider to disclose covered personal data if a court
 19 order would be required for the governmental entity
 20 to require an online service provider to disclose such
 21 covered personal data that is a record of a customer
 22 or subscriber of the online service provider.

23 “(3) ORDERS.—

24 “(A) IN GENERAL.—A court may only
 25 issue an order requiring a covered organization

1 that is not an online service provider to disclose
 2 covered personal data on the same basis and
 3 subject to the same limitations as would apply
 4 to a court order to require disclosure by an on-
 5 line service provider.

6 “(B) STANDARD.—For purposes of sub-
 7 paragraph (A), a court shall apply the most
 8 stringent standard under Federal statute or the
 9 Constitution of the United States that would be
 10 applicable to a request for a court order to re-
 11 quire a comparable disclosure by an online serv-
 12 ice provider of a customer or subscriber of the
 13 online service provider.”.

14 **SEC. 505. PROTECTION OF DATA ENTRUSTED TO INTER-**
 15 **MEDIARY OR ANCILLARY SERVICE PRO-**
 16 **VIDERS.**

17 (a) DEFINITION.—Section 2711 of title 18, United
 18 States Code, as amended by section 503 of this Act, is
 19 amended by adding at the end the following:

20 “(6) the term ‘intermediary or ancillary service
 21 provider’ means an entity or facilities owner or oper-
 22 ator that directly or indirectly delivers, transmits,
 23 stores, or processes communications or any other
 24 covered personal data (as defined in section 2702(e))

1 of this title) for, or on behalf of, an online service
2 provider.”.

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

5 (1) in paragraph (1), by striking “and” at the
6 end;

7 (2) in paragraph (2)(B), by striking “and” at
8 the end;

9 (3) in paragraph (3), by striking the period at
10 the end and inserting “; and”; and

11 (4) by adding at the end the following:

12 “(4) an intermediary or ancillary service pro-
13 vider may not knowingly disclose—

14 “(A) to any person or entity the contents
15 of a communication while in electronic storage
16 by that intermediary or ancillary service pro-
17 vider; or

18 “(B) to any governmental entity a record
19 or other information pertaining to a subscriber
20 to or customer of, a recipient of a communica-
21 tion from a subscriber to or customer of, or the
22 sender of a communication to a subscriber to or
23 customer of, the online service provider for, or
24 on behalf of, which the intermediary or ancil-
25 lary service provider directly or indirectly deliv-

1 ers, transmits, stores, or processes communica-
 2 tions or any other covered personal data (as de-
 3 fined in subsection (e)).”.

4 **TITLE VI—TRANSPARENCY**

5 **SEC. 601. ENHANCED REPORTS BY DIRECTOR OF NATIONAL** 6 **INTELLIGENCE.**

7 (a) IN GENERAL.—Section 603(b) of the Foreign In-
 8 telligence Surveillance Act of 1978 (50 U.S.C. 1873(b))
 9 is amended—

10 (1) in paragraph (2)(C), by striking the semi-
 11 colon and inserting “; and”;

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

14 (3) by inserting after paragraph (2) the fol-
 15 lowing:

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

18 “(4) statistics revealing the number of persons
 19 targeted and the number of selectors used under sec-
 20 tion 702(a), disaggregated by the certification under
 21 which the person was targeted;

22 “(5) the total number of directives issued pur-
 23 suant to section 702(i)(1), disaggregated by each
 24 type of electronic communication service provider de-
 25 scribed in section 701(b)(4);”;

1 (4) in paragraph (9), as so redesignated, by
2 striking “and” at the end;

3 (5) in paragraph (10), as so redesignated, by
4 striking the period at the end and inserting a semi-
5 colon; and

6 (6) by adding at the end the following:

7 “(11)(A) the total number of disseminated in-
8 telligence reports derived from collection pursuant to
9 section 702 containing the identities of United
10 States persons, regardless of whether the identities
11 of the United States persons were openly included or
12 masked;

13 “(B) the total number of disseminated intel-
14 ligence reports derived from collection not authorized
15 by this Act and conducted under procedures ap-
16 proved by the Attorney General containing the iden-
17 tities of United States persons, regardless of wheth-
18 er the identities of the United States persons were
19 openly included or masked;

20 “(C) the total number of disseminated intel-
21 ligence reports derived from collection pursuant to
22 section 702 containing the identities of United
23 States persons in which the identities of the United
24 States persons were masked;

1 “(D) the total number of disseminated intel-
2 ligence reports derived from collection not authorized
3 by this Act and conducted under procedures ap-
4 proved by the Attorney General containing the iden-
5 tities of United States persons in which the identi-
6 ties of the United States persons were masked;

7 “(E) the total number of disseminated intel-
8 ligence reports derived from collection pursuant to
9 section 702 containing the identities of United
10 States persons in which the identities of the United
11 States persons were openly included; and

12 “(F) the total number of disseminated intel-
13 ligence reports derived from collection not authorized
14 by this Act and conducted under procedures ap-
15 proved by the Attorney General containing the iden-
16 tities of United States persons in which the identi-
17 ties of the United States persons were openly in-
18 cluded;

19 “(12) the number of queries conducted in an ef-
20 fort to find communications or information of or
21 about 1 or more United States persons or persons
22 reasonably believed to be located in the United
23 States at the time of the query or the time of the
24 communication or creation of the information, where
25 such communications or information were obtained

1 under procedures approved by the Attorney General
2 and without a court order, subpoena, or other legal
3 process established by statute;

4 “(13) the number of criminal proceedings in
5 which the Federal Government or a government of
6 a State or political subdivision thereof entered into
7 evidence or otherwise used or disclosed in a criminal
8 proceeding any information obtained or derived from
9 an acquisition conducted under procedures approved
10 by the Attorney General and without a court order,
11 subpoena, or other legal process established by stat-
12 ute; and

13 “(14) a good faith estimate of what percentage
14 of the communications that are subject to the proce-
15 dures described in section 309(b)(3) of the Intel-
16 ligence Authorization Act for Fiscal Year 2015 (50
17 U.S.C. 1813(b)(3))—

18 “(A) are retained for more than 5 years;

19 and

20 “(B) are retained for more than 5 years

21 because, in whole or in part, the communica-
22 tions are encrypted.”.

23 (b) REPEAL OF NONAPPLICABILITY TO FEDERAL
24 BUREAU OF INVESTIGATION OF CERTAIN REQUIRE-

1 MENTS.—Section 603(d) of the Foreign Intelligence Sur-
 2 veillance Act of 1978 (50 U.S.C. 1873(d)) is amended—

3 (1) by striking paragraph (2); and

4 (2) by redesignating paragraph (3) as para-
 5 graph (2).

6 (c) CONFORMING AMENDMENT.—Section 603(d)(1)
 7 of the Foreign Intelligence Surveillance Act of 1978 (50
 8 U.S.C. 1873(d)(1)) is amended by striking “paragraphs
 9 (3), (5), or (6)” and inserting “paragraph (6), (8), or
 10 (9)”.

11 **SEC. 602. NOTIFICATION TO CONGRESS OF CERTAIN UNAU-**
 12 **THORIZED DISCLOSURES.**

13 Section 18(a) of the Reforming Intelligence and Se-
 14 curing America Act (50 U.S.C. 1881a note) is amended
 15 by striking “congressional intelligence committees” and
 16 inserting “appropriate congressional committees”.

17 **TITLE VII—LIMITED DELAYS IN**
 18 **IMPLEMENTATION**

19 **SEC. 701. LIMITED DELAYS IN IMPLEMENTATION.**

20 (a) DEFINITION.—In this section, the term “appro-
 21 priate committees of Congress” means—

22 (1) the congressional intelligence committees
 23 (as defined in section 3 of the National Security Act
 24 of 1947 (50 U.S.C. 3003));

1 (2) the Committee on the Judiciary of the Sen-
2 ate; and

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

5 (b) AUTHORITY.—The Attorney General may, in co-
6 ordination with the Director of National Intelligence as
7 may be appropriate, delay implementation of a provision
8 of this Act or an amendment made by this Act for a period
9 of not more than 180 days upon a showing to the appro-
10 priate committees of Congress that the delay is nec-
11 essary—

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

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

Calendar No. 371

119TH CONGRESS
2D Session
S. 4280

A BILL

To amend the Foreign Intelligence Surveillance Act of 1978 to reauthorize and reform certain authorities and to provide greater transparency and oversight.

APRIL 14, 2026

Read the second time and placed on the calendar