**AMENDMENT TO THE AMENDMENT IN THE NATURE OF A SUBSTITUTE TO H.R. 6570**
**OFFERED BY MR. BIGGS OF ARIZONA**

At the end of the bill, add the following:

## SEC. 23. DEFINITIONS.

In Sections 23 through 27:

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

(2) ELECTRONIC SURVEILLANCE, PERSON, STATE, UNITED STATES, AND UNITED STATES PERSON.—The terms "electronic surveillance", "person", "State", "United States", and "United States person" have the meanings given such terms in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

## SEC. 24. PROHIBITION ON WARRANTLESS QUERIES FOR THE COMMUNICATIONS OF UNITED STATES PERSONS AND PERSONS LOCATED IN THE UNITED STATES.

(a) In General.—Except as provided in subsections (b) and (c), no officer or employee of the Federal Government may conduct a query of information acquired pursuant to Executive Order 12333 (50 U.S.C. 3001 note; relating to United States intelligence activities), or successor order, in an effort to find communications or information the compelled production of which would require a probable cause warrant if sought for law enforcement purposes in the United States of or about 1 or more United States persons or persons reasonably believed to be located in the United States at the time of the query or the time of the communication or creation of the information.

(b) Concurrent Authorization, Consent, and Exception for Emergency Situations.—

(1) IN GENERAL.—Subsection (a) shall not apply to a query relating to United States person or persons reasonably believed to be located in the United States at the time of the query or the time of the communication or creation of the information if—

(A) such persons or person are the subject of an order or emergency authorization authorizing electronic surveillance or physical search under section 105 or 304 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805, 1824 ), or a warrant issued pursuant to the Federal Rules of Criminal Procedure by a court of competent jurisdiction covering the period of the query;

(B)(i) the officer or employee carrying out the query has a reasonable belief that—

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

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

(ii) a description of the query is provided to the congressional intelligence committees (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)) in a timely manner;

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

(D)(i) the query uses a known cybersecurity threat signature as a query term;

(ii) the query is conducted, and the results of the query are used, for the sole purpose of identifying targeted recipients of malicious software and preventing or mitigating harm from such malicious software;

(iii) no additional contents of communications retrieved as a result of the query are accessed or reviewed; and

(iv) all such queries are reported to the Foreign Intelligence Surveillance Court.

(2) LIMITATIONS.—

(A) USE IN SUBSEQUENT PROCEEDINGS AND INVESTIGATIONS.—No information retrieved pursuant to a query authorized by paragraph (1)(B) or evidence derived from such query may be used, received in evidence, or otherwise disseminated in any investigation, trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, except in a proceeding or investigation that arises from the threat that prompted the query.

(B) ASSESSMENT OF COMPLIANCE.—Not less frequently than annually, the Attorney General shall assess compliance with the requirements under subparagraphs (A).

(c) Matters Relating to Emergency Queries.—

(1) TREATMENT OF DENIALS.—In the event that a query for communications or information the compelled production of which would require a probable cause warrant if sought for law enforcement purposes in the United States relating to 1 or more United States persons or persons reasonably believed to be located in the United States at the time of the query or the time of communication, or creation of the information is conducted pursuant to an emergency authorization described in subsection (b)(1)(A) and the application for such emergency authorization is denied, or in any other case in which the query has been conducted and no order is issued approving the query—

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

(B) no information concerning any United States person or person reasonably believed to be located in the United States at the time of acquisition or the time of

communication or creation of the information acquired from such query may subsequently be used or disclosed in any other manner without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

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

(d) Foreign Intelligence Surveillance Act of 1978.—This section shall not apply to queries of communications and information collected pursuant to the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

(e) Foreign Intelligence Purpose.—Except as provided in subsection (b)(1), no officer or employee of the United States may conduct a query of information acquired pursuant to Executive Order 12333 (50 U.S.C. 3001 note; relating to United States intelligence activities), or successor order, in an effort to find information of our about 1 or more United States persons or persons reasonably believed to be located in the United States at the time of the query or the time of communication or creation of the information unless the query is reasonably likely to retrieve foreign intelligence information.

(f) Documentation.—No officer or employee of the Federal Government may conduct a query of information acquired pursuant to Executive Order 12333 (50 U.S.C. 3001 note; relating to United States intelligence activities), or successor order, in an effort to find information of or about 1 or more United States persons or persons reasonably believed to be located in the United States at the time of the query or the time of the communication or creation of the information unless first an electronic record is created, and a system, mechanism, or business practice is in place to maintain such record, that includes the following:

(1) Each term used for the conduct of the query.

(2) The date of the query.

(3) The identifier of the officer or employee.

(4) A statement of facts showing that the use of each query term included under paragraph (1) is reasonably likely to retrieve foreign intelligence information.

(g) Prohibition on Results of Metadata Query as a Basis for Access to Communications and Other Protected Information.—If a query of information is conducted in an effort to find communications metadata of 1 or more United States persons or persons reasonably believed to be located in the United States at the time of acquisition or communication and the query returns such information, the results of the query may not be used as a basis for reviewing communications or information a query for which is otherwise prohibited under this sections.

## SEC. 25. PROHIBITION ON REVERSE TARGETING OF UNITED STATES PERSONS AND PERSONS LOCATED IN THE UNITED STATES.

(a) Prohibition on Acquisition.—

(1) PROHIBITION WITH EXCEPTIONS.—No officer or employee of the United States may intentionally target, pursuant to Executive Order 12333 (50 U.S.C. 3001 note; relating to United States intelligence activities), or successor order, any person if a significant purpose of the acquisition is to target 1 or more United States persons or persons reasonably

believed to be located in the United States at the time of acquisition, communication, or the creation of the information as prohibited by Section 703 of the Foreign Intelligence Surveillance Act of 1978, as added by section 201 of this Act, unless—

(A)(i) there is a reasonable belief that an emergency exists involving a threat of imminent death or serious bodily harm to such United States person or person reasonably believed to be in the United States at the time of the query or the time of acquisition or communication;

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

(iii) a description of the targeting is provided to the congressional intelligence committees (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)) in a timely manner; or

(B) the United States person or persons reasonably believed to be located in the United States at the time of acquisition, communication or creation of the information has provided consent to the targeting, or if such person is incapable of providing consent, a third party legally authorized to consent on behalf of such person has provided consent.

(2) LIMITATION ON EXCEPTION.—No information acquired pursuant to paragraph (1)(A) or evidence derived from such targeting may be used, received in evidence, or otherwise disseminated in any investigation, trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, except in proceedings or investigations that arise from the threat that prompted the targeting.

(b) Foreign Intelligence Surveillance Act of 1978 and Criminal Warrants.—This section shall not apply to—

(1) an acquisition carried out pursuant to both section 702 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881a), as amended by section 103 of this Act, and section 703(b)(2) of the Foreign Intelligence Surveillance Act of 1978, as added by section 201 of this Act;

(2) an acquisition authorized under section 105 or 304 of the Foreign Intelligence Surveillance act of 1978 (50 U.S.C. 1805 and 1824); or

(3) an acquisition pursuant to a warrant issued pursuant to the Federal Rules of Criminal Procedure.

## SEC. 26. PROHIBITION ON THE WARRANTLESS ACQUISITION OF DOMESTIC COMMUNICATIONS.

(a) In General.—No officer or employee of the United States may intentionally acquire pursuant to Executive Order 12333 (50 U.S.C. 3001 note; relating to United States intelligence activities), or successor order, any communication as to which the sender and all intended recipients are known to be located in the United States at the time of acquisition or the time of communication except—

(1) as authorized under section 105 or 304 the Foreign Intelligence Surveillance Act of

1978 (50 U.S.C. 1805 and 1824); or

(2) if—

(A) there is a reasonable belief that—

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

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

(B) a description of the acquisition is provided to the congressional intelligence committees (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)) in a timely manner.

(b) Use in Subsequent Proceedings and Investigations.—No information acquired pursuant to an emergency described in subsection (a)(2) or information derived from such acquisition may be used, received in evidence, or otherwise disseminated in any investigation, trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, except in a proceeding or investigation that arises from the threat that prompted the acquisition.

## SEC. 27. DATA RETENTION LIMITS.

(a) Procedures.—Each head of an element of the Intelligence Community shall develop and implement procedures governing the retention of information collected pursuant to Executive Order 12333 (50 U.S.C. 3001 note; relating to United States intelligence activities), or successor order.

(b) Requirements.—

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

(A) any information, including an encrypted communication, to, from, or pertaining to a United States person or person reasonably believed to be located in the United States at the time of acquisition, communication, or creation of the information that has been evaluated and is not specifically known to contain foreign intelligence information; and

(B) any unevaluated information, unless it can reasonably be determined that the unevaluated information does not contain communications to or from, or information pertaining to a United States person or person reasonably believed to be located in the United States at the time of acquisition, communication, or creation of the information.

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

(A) the information is the subject of a preservation obligation in pending

administrative, civil, or criminal litigation, in which case the covered information shall be segregated, retained, and used solely for that purpose and shall be destroyed as soon as it is no longer required to be preserved for such litigation; or

(B) the information is being used in a proceeding or investigation in which the information is directly related to and necessary to address a specific threat identified in section 706(a)(2)(B) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881e(a)(2)(B)), as amended by section 102.