(2) recognizes the valiant search efforts of the members of the Coast Guard, Navy, and Air Force who searched for the crew members of the *El Faro*; and

(3) offers heartfelt condolences to the family, friends, and loved ones of the crew members of the *El Faro*.

AMENDMENTS SUBMITTED AND PROPOSED

SA 2720. Mr. GARDNER submitted an amendment intended to be proposed to amendment SA 2716 proposed by Mr. BURR (for himself and Mrs. FEINSTEIN) to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table.

SA 2721. Mr. GARDNER submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2722. Mr. GARDNER submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2723. Mr. LEAHY (for himself and Mr. LEE) submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2724. Mr. THUNE submitted an amendment intended to be proposed to amendment SA 2716 proposed by Mr. BURR (for himself and Mrs. FEINSTEIN) to the bill S. 754, supra; which was ordered to lie on the table.

SA 2725. Mr. THUNE submitted an amendment intended to be proposed to amendment SA 2716 proposed by Mr. BURR (for himself and Mrs. FEINSTEIN) to the bill S. 754, supra; which was ordered to lie on the table.

SA 2726. Mr. THUNE submitted an amendment intended to be proposed to amendment SA 2716 proposed by Mr. BURR (for himself and Mrs. FEINSTEIN) to the bill S. 754, supra; which was ordered to lie on the table.

SA 2727. Mr. THUNE submitted an amendment intended to be proposed to amendment SA 2716 proposed by Mr. BURR (for himself and Mrs. FEINSTEIN) to the bill S. 754, supra; which was ordered to lie on the table.

SA 2728. Mr. THUNE submitted an amendment intended to be proposed to amendment SA 2716 proposed by Mr. BURR (for himself and Mrs. FEINSTEIN) to the bill S. 754, supra; which was ordered to lie on the table.

SA 2729. Mr. THUNE submitted an amendment intended to be proposed to amendment SA 2716 proposed by Mr. BURR (for himself and Mrs. FEINSTEIN) to the bill S. 754, supra; which was ordered to lie on the table.

SA 2730. Mr. THUNE submitted an amendment intended to be proposed to amendment SA 2716 proposed by Mr. BURR (for himself and Mrs. FEINSTEIN) to the bill S. 754, supra; which was ordered to lie on the table.

SA 2731. Ms. AYOTTE (for Mr. GRAHAM) submitted an amendment intended to be proposed by Ms. Ayotte to the bill S. 754, supra; which was ordered to lie on the table.

SA 2732. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2733. Mr. BLUMENTHAL submitted an amendment intended to be proposed to amendment SA 2716 proposed by Mr. BURR (for himself and Mrs. FEINSTEIN) to the bill S. 754, supra; which was ordered to lie on the table.

SA 2734. Mr. BLUMENTHAL submitted an amendment intended to be proposed to amendment SA 2716 proposed by Mr. BURR (for himself and Mrs. FEINSTEIN) to the bill S. 754, supra; which was ordered to lie on the table.

SA 2735. Mr. MANCHIN submitted an amendment intended to be proposed to amendment SA 2716 proposed by Mr. BURR (for himself and Mrs. FEINSTEIN) to the bill S. 754, supra; which was ordered to lie on the table.

SA 2736. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table .

SA 2737. Mr. MANCHIN submitted an amendment intended to be proposed to amendment SA 2716 proposed by Mr. BURR (for himself and Mrs. FEINSTEIN) to the bill S. 754, supra; which was ordered to lie on the table.

SA 2738. Mr. BOOKER (for himself and Mr. HELLER) submitted an amendment intended to be proposed to amendment SA 2716 proposed by Mr. BURR (for himself and Mrs. FEINSTEIN) to the bill S. 754, supra; which was ordered to lie on the table.

SA 2739. Mr. REED submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2740. Mr. SULLIVAN submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2741. Mr. SULLIVAN submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2742. Mr. CARPER submitted an amendment intended to be proposed to amendment SA 2716 proposed by Mr. BURR (for himself and Mrs. FEINSTEIN) to the bill S. 754, supra; which was ordered to lie on the table.

SA 2743. Mr. BURR submitted an amendment intended to be proposed to amendment SA 2716 proposed by Mr. BURR (for himself and Mrs. FEINSTEIN) to the bill S. 754, supra; which was ordered to lie on the table.

SA 2744. Mr. LEAHY (for himself and Mr. GRASSLEY) submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2745. Mr. FRANKEN (for himself and Mr. LEAHY) submitted an amendment intended to be proposed to amendment SA 2716 proposed by Mr. BURR (for himself and Mrs. FEINSTEIN) to the bill S. 754, supra; which was ordered to lie on the table.

SA 2746. Mr. BURR submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2747. Mr. VITTER proposed an amendment to the bill H.R. 208, to improve the disaster assistance programs of the Small Business Administration.

TEXT OF AMENDMENTS

SA 2720. Mr. GARDNER submitted an amendment intended to be proposed to amendment SA 2716 proposed by Mr. BURR (for himself and Mrs. FEINSTEIN) to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 16, line 9, insert ''make reasonable efforts to'' before ''review''.

On page 16, line 11, strike ''knows'' and insert ''reasonably believes''.

On page 16, line 17, insert ''identify and'' before ''remove''.

On page 16, line 19, strike ''knows'' and insert ''reasonably believes''.

SA 2721. Mr. GARDNER submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. REPORT ON ACCOUNTABILITY FOR THE DATA BREACH OF THE OFFICE OF PERSONNEL MANAGEMENT.

(a) DEFINITIONS.—In this section:

(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term ''appropriate committees of Congress'' means—

(A) the Committee on Foreign Relations, the Select Committee on Intelligence, and the Committee on Homeland Security and Governmental Affairs of the Senate; and

(B) the Committee on Foreign Affairs, the Committee on Homeland Security, and the Permanent Select Committee on Intelligence of the House of Representatives.

(2) DATA BREACH.—The term ''data breach'' means the data breach of systems of the Office of Personnel Management that occurred during fiscal year 2015 which resulted in the theft of sensitive information of at least 21,500,000 Federal employees and their families.

(b) REQUIREMENT FOR REPORT.—Not later than 30 days after date of the enactment of this Act, the President shall submit to the appropriate committees of Congress and make available to the public a report that—

(1) identifies the perpetrator, including any state sponsor, of the data breach;

(2) includes a plan to impose penalties on such perpetrator under United States law; and

(3) describes a strategy to initiate diplomatic discussions with any state sponsor of the data breach.

(c) ELEMENTS.—The report required by subsection (a) shall include the following:

(1) Identification of any individual perpetrator of the data breach, by name and nationality.

(2) Identification of any state sponsor of the data breach, including each agency of the government of the state sponsor that was responsible for authorizing, performing, or endorsing the data breach.

(3) A description of the actions proposed to penalize each individual identified under paragraph (1) under United States law.

(4) The strategy required by subsection (a)(3) shall include—

(A) a description of any action the President has undertaken to initiate or carry out diplomatic discussions with any state sponsor identified under paragraph (2); and

(B) a strategy to initiate or carry out diplomatic discussions in high-level forums and interactions during the 180-day period beginning on the date of the enactment of this Act.

SA 2722. Mr. GARDNER submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. BIENNIAL CYBER REVIEW.

(a) REQUIREMENT FOR REVIEW.—Beginning in 2016 and not less frequently than once every two years thereafter, the President shall complete a review of the cyber posture of the United States, including an unclassified summary of roles, missions, accomplishments, plans, and programs.

(b) PURPOSES.—The purposes of each such review are—

(1) to assess the cyber security of the United States;

(2) to determine and express the cyber strategy of the United States; and

(3) to establish a revised cyber program for the next 2-year period.

(c) CONTENT.—Each review required by subsection (a) shall include—

(1) a comprehensive examination of the cyber strategy, force structure, personnel, modernization plans, infrastructure, and budget plan of the United States;

(2) an assessment of the ability of the United States to recover from a cyber emergency;

(3) an assessment of other elements of the cyber program of the United States;

(4) an assessment of critical national security infrastructure and data that is vulnerable to cyberattacks and cybertheft; and

(5) an assessment of international engagement efforts to establish viable norms of behavior in cyberspace to implement the 2011 International Strategy for Cyberspace.

(d) INVOLVEMENT OF CYBERSECURITY ADVISORY PANEL.—

(1) REQUIREMENT TO INFORM.—The President shall inform the Cybersecurity Advisory Panel established or designated under section _____, on an ongoing basis, of the actions carried out to conduct each review required by subsection (a).

(2) ASSESSMENT PRIOR TO COMPLETION OF REVIEW.—Not later than 1 year prior to the date of completion of each review required by subsection (a), the Chairman of the Cybersecurity Advisory Panel shall submit to the President, the assessment of such Panel of actions carried out to conduct the review as of the date of the submission, including any recommendations of the Panel for improvements to the review or for additional matters to be covered in the review.

(3) ASSESSMENT OF COMPLETED REVIEW.—At the time each review required by subsection (a) is completed and in time to be included in a report required by subsection (d), the Chairman of the Cybersecurity Advisory Panel shall submit to the President, on behalf of the Panel, an assessment of such review.

(e) REPORT.—Not later than September 30, 2016, and not less frequently than once every two years thereafter, the President shall submit to Congress a comprehensive report on each review required by subsection (a). Each report shall include—

(1) the results of the review, including a comprehensive discussion of the cyber strategy of the United States and the collaboration between the public and private sectors best suited to implement that strategy;

(2) a description of the threats examined for purposes of the review and the scenarios developed in the examination of such threats;

(3) the assumptions used in the review, including assumptions relating to the cooperation of other countries and levels of acceptable risk; and

(4) the assessment of the Cybersecurity Advisory Panel submitted under subsection (c)(3).

SEC. _____. CYBERSECURITY ADVISORY PANEL.

(a) IN GENERAL.—The President shall establish or designate a Cybersecurity Advisory Panel.

(b) APPOINTMENT.—The President—

(1) shall appoint as members of the Cybersecurity Advisory Panel representatives of industry, academic, nonprofit organizations, interest groups, and advocacy organizations, and State and local governments who are qualified to provide advice and information on cybersecurity research, development, demonstrations, education, personnel, technology transfer, commercial application, or societal and civil liberty concerns;

(2) shall appoint a Chairman of the Panel from among the members of the Panel; and

(3) may seek and give consideration to recommendations for appointments to the Panel from Congress, industry, the cybersecurity community, the defense community, State and local governments, and other appropriate organizations.

(c) DUTIES.—The Cybersecurity Advisory Panel shall advise the President on matters relating to the national cybersecurity program and strategy and shall assess—

(1) trends and developments in cybersecurity science research and development;

(2) progress made in implementing the strategy;

(3) the need to revise the strategy;

(4) the readiness and capacity of the Federal and national workforces to implement the national cybersecurity program and strategy, and the steps necessary to improve workforce readiness and capacity;

(5) the balance among the components of the national strategy, including funding for program components;

(6) whether the strategy, priorities, and goals are helping to maintain United States leadership and defense in cybersecurity;

(7) the management, coordination, implementation, and activities of the strategy;

(8) whether the concerns of Federal, State, and local law enforcement entities are adequately addressed; and

(9) whether societal and civil liberty concerns are adequately addressed.

(d) REPORTS.—Not less frequently than once every 4 years, the Cybersecurity Advisory Panel shall submit to the President a report on its assessments under subsection (c) and its recommendations for ways to improve the strategy.

(e) TRAVEL EXPENSES OF NON-FEDERAL MEMBERS.—Non-Federal members of the Cybersecurity Advisory Panel, while attending meetings of the Panel or while otherwise serving at the request of the head of the Panel while away from their homes or regular places of business, may be allowed travel expenses, including per diem in lieu of subsistence, as authorized by section 5703 of title 5, United States Code, for individuals in the Government serving without pay. Nothing in this subsection shall be construed to prohibit members of the Panel who are officers or employees of the United States from being allowed travel expenses, including per diem in lieu of subsistence, in accordance with law.

(f) EXEMPTION FROM FACA SUNSET.—Section 14 of the Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to the Cybersecurity Advisory Panel.

SA 2723. Mr. LEAHY (for himself and Mr. LEE) submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the end, add the following:

SEC. 408. AUDIT OF USE OF DEA ADMINISTRATIVE SUBPOENA AUTHORITY.

(a) AUDIT.—The Inspector General of the Department of Justice shall perform an audit of the effectiveness and use, including any improper or illegal use, of subpoenas issued pursuant to section 506 of the Controlled Substances Act (21 U.S.C. 876).

(b) REQUIREMENTS.—The audit required under subsection (a) shall include—

(1) an examination of the use of subpoenas issued pursuant to section 506 of the Controlled Substances Act (21 U.S.C. 876) during calendar years 2012 through 2014;

(2) a description of any noteworthy facts or circumstances relating to such use, including any improper or illegal use of such authority; and

(3) an examination of the effectiveness of subpoenas issued pursuant to section 506 of the Controlled Substances Act (21 U.S.C. 876) as an investigative tool, including—

(A) the manner in which information acquired pursuant to such subpoenas is collected, retained, analyzed, and disseminated by the Department of Justice, including any direct access to such information (such as access to raw data) provided to any other department, agency, or instrumentality of the Federal Government, State, local, or tribal governments, or any private sector entity;

(B) whether, and how often, such information was used in civil and criminal proceedings; and

(C) whether, and how often, the Department of Justice used such information to produce an analytical intelligence product for distribution within the Department of Justice to the intelligence community (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)) or to any other department, agency, or instrumentality of the Federal Government or of a State, local, or tribal government.

(c) SUBMISSION DATES.—

(1) PRIOR YEARS.—The Inspector General of the Department of Justice shall submit to the Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives a report containing the results of the audit conducted under this section for calendar years 2012 through 2014 not later than the earlier of—

(A) 1 year after the date of enactment of this Act; or

(B) the date on which the audit required under this section for calendar years 2012 through 2014 is completed.

(2) CALENDAR YEARS 2015 THROUGH 2017.—The Inspector General of the Department of Justice shall submit to the Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives a report containing the results of the audit conducted under this section for calendar years 2015 through 2017 not later than the earlier of—

(A) December 31, 2018; or

(B) the date on which the audit required under this section for calendar years 2015 through 2017 is completed.

(3) DELAY OF EXISTING REVIEWS PROHIBITED.—The Inspector General of the Department of Justice shall not delay the completion of any review commenced before the date of enactment of this Act pertaining to subpoenas issued pursuant to section 506 of the Controlled Substances Act (21 U.S.C. 876) pending the completion of the reports required by this section.

SA 2724. Mr. THUNE submitted an amendment intended to be proposed to amendment SA 2716 proposed by Mr. BURR (for himself and Mrs. FEINSTEIN) to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 86, line 26, insert ''the Director of the National Institute of Standards and Technology and'' after ''in coordination with''.

SA 2725. Mr. THUNE submitted an amendment intended to be proposed to amendment SA 2716 proposed by Mr. BURR (for himself and Mrs. FEINSTEIN) to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 89, line 23, insert '', the Director of the National Institute of Standards and Technology,'' after ''Director''.

SA 2726. Mr. THUNE submitted an amendment intended to be proposed to amendment SA 2716 proposed by Mr. BURR (for himself and Mrs. FEINSTEIN) to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 91, line 21, insert '', in consultation with the Director of the National Institute of Standards and Technology,'' after ''Security''.

SA 2727. Mr. THUNE submitted an amendment intended to be proposed to amendment SA 2716 proposed by Mr. BURR (for himself and Mrs. FEINSTEIN) to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 92, line 9, insert '', in consultation with the Director of the National Institute of Standards and Technology,'' after ''Secretary''.

SA 2728. Mr. THUNE submitted an amendment intended to be proposed to amendment SA 2716 proposed by Mr. BURR (for himself and Mrs. FEINSTEIN) to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 103, line 12, insert ''the Director of the National Institute of Standards and Technology and'' after ''consultation with''.

SA 2729. Mr. THUNE submitted an amendment intended to be proposed to amendment SA 2716 proposed by Mr. BURR (for himself and Mrs. FEINSTEIN) to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 111, strike lines 21 through 24, and insert the following:

(E) the Committee on Energy and Natural Resources of the Senate;

(F) the Committee on Energy and Commerce of the House of Representatives; and

(G) the Committee on Commerce, Science, and Transportation of the Senate.

SA 2730. Mr. THUNE submitted an amendment intended to be proposed to amendment SA 2716 proposed by Mr. BURR (for himself and Mrs. FEINSTEIN) to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 85, strike lines 12 through 20, and insert the following:

(D) the Committee on Commerce, Science, and Transportation of the Senate;

(E) the Committee on Armed Services of the House of Representatives;

(F) the Committee on Homeland Security of the House of Representatives;

(G) the Committee on Oversight and Government Reform of the House of Representatives; and

(H) the Permanent Select Committee on Intelligence of the House of Representatives.

SA 2731. Ms. AYOTTE (for Mr. GRAHAM) submitted an amendment intended to be proposed by Ms. AYOTTE to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ___. SENSE OF THE SENATE.

It is the Sense of the Senate that the Memorandum Opinion for the Assistant Attorney General dated September 20, 2011, does not carry the force of law and the Senate is concerned with the cybersecurity implications of activities undertaken in reliance of such Opinion, including the potential for thefts of personally identifiable information, and the participation in such activities by entities, including successors of such entities, charged or sued by the Government with respect to such activities, with a violation of subchapter IV of chapter 53 of title 31, United States Code, or any other Federal statute relating to monetary transactions.

SA 2732. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the end, add the following:

TITLE V—OTHER MATTERS

SEC. 501. EXPANSION OF CHOICE PROGRAM OF DEPARTMENT OF VETERANS AFFAIRS.

(a) ELIMINATION OF SUNSET.—

(1) IN GENERAL.—Section 101 of the Veterans Access, Choice, and Accountability Act of 2014 (Public Law 113–146; 38 U.S.C. 1701 note) is amended—

(A) by striking subsection (p); and

(B) by redesignating subsections (q), (r), (s), and (t) as subsections (p), (q), (r), and (s), respectively.

(2) CONFORMING AMENDMENTS.—Such section is amended—

(A) in subsection (i)(2), by striking ''during the period in which the Secretary is authorized to carry out this section pursuant to subsection (p)''; and

(B) in subsection (p)(2), as redesignated by paragraph (1)(B), by striking subparagraph (F).

(b) EXPANSION OF ELIGIBILITY.—

(1) IN GENERAL.—Subsection (b) of such section is amended to read as follows:

''(b) ELIGIBLE VETERANS.—A veteran is an eligible veteran for purposes of this section if the veteran is enrolled in the patient enrollment system of the Department of Veterans Affairs established and operated under section 1705 of title 38, United States Code, including any such veteran who has not received hospital care or medical services from the Department and has contacted the Department seeking an initial appointment from the Department for the receipt of such care or services.''.

(2) CONFORMING AMENDMENTS.—Such section is amended—

(A) in subsection (c)(1)—

(i) in the matter preceding subparagraph (A), by striking ''In the case of an eligible veteran described in subsection (b)(2)(A), the Secretary shall, at the election of the eligible veteran'' and inserting ''The Secretary shall, at the election of an eligible veteran''; and

(ii) in subparagraph (A), by striking ''described in such subsection'' and inserting ''of the Veterans Health Administration'';

(B) in subsection (f)(1), by striking ''subsection (b)(1)'' and inserting ''subsection (b)'';

(C) in subsection (g), by striking paragraph (3); and

(D) in subsection (p)(2)(A), as redesignated by subsection (a)(1)(B), by striking '', disaggregated by—'' and all that follows through ''subsection (b)(2)(D)''.

(c) EFFECTIVE DATE.—The amendments made by this section shall apply with respect to hospital care and medical services furnished under section 101 of the Veterans Access, Choice, and Accountability Act of 2014 (Public Law 113–146; 38 U.S.C. 1701 note) on and after the date that is 90 days after the date of the enactment of this Act.

SA 2733. Mr. BLUMENTHAL submitted an amendment intended to be proposed to amendment SA 2716 proposed by Mr. BURR (for himself and Mrs. FEINSTEIN) to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 48, between lines 6 and 7, insert the following:

(c) PRIVATE RIGHT OF ACTION FOR VIOLATIONS BY FEDERAL ENTITIES OF RESTRICTIONS ON DISCLOSURE, USE, AND PROTECTION OF VOLUNTARILY SHARED CYBER THREAT INDICATORS.—

(1) IN GENERAL.—If a department or agency of the Federal Government knowingly or recklessly violates the requirements of this Act with respect to the disclosure, use, or protection of voluntarily shared cyber threat indicators, the United States shall be liable to a person adversely affected by such violation in an amount equal to the sum of—

(A) the actual damages sustained by the person as a result of the violation or $50,000, whichever is greater; and

(B) the costs of the action together with reasonable attorney fees as determined by the court.

(2) VENUE.—An action to enforce liability created under this subsection may be brought in the district court of the United States in—

(A) the district in which the complainant resides;

(B) the district in which the principal place of business of the complainant is located;

(C) the district in which the department or agency of the Federal Government that disclosed the information is located; or

(D) the District of Columbia.

(3) STATUTE OF LIMITATIONS.—No action shall lie under this subsection unless such

action is commenced not later than two years after the person adversely affected by a violation described in paragraph (1) first learns, or by which such person reasonably should have learned, of the facts and circumstances giving rise to the action.

SA 2734. Mr. BLUMENTHAL submitted an amendment intended to be proposed to amendment SA 2716 proposed by Mr. BURR (for himself and Mrs. FEINSTEIN) to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 47, between lines 7 and 8, insert the following:

(c) PRIVATE RIGHT OF ACTION FOR VIOLATIONS BY FEDERAL ENTITIES OF RESTRICTIONS ON DISCLOSURE, USE, AND PROTECTION OF VOLUNTARILY SHARED CYBER THREAT INDICATORS.—

(1) IN GENERAL.—If a department or agency of the Federal Government knowingly or recklessly violates the requirements of this Act with respect to the disclosure, use, or protection of voluntarily shared cyber threat indicators, the United States shall be liable to a person adversely affected by such violation in an amount equal to the sum of—

(A) the actual damages sustained by the person as a result of the violation or $1,000, whichever is greater; and

(B) the costs of the action together with reasonable attorney fees as determined by the court.

(2) VENUE.—An action to enforce liability created under this subsection may be brought in the district court of the United States in—

(A) the district in which the complainant resides;

(B) the district in which the principal place of business of the complainant is located;

(C) the district in which the department or agency of the Federal Government that disclosed the information is located; or

(D) the District of Columbia.

(3) STATUTE OF LIMITATIONS.—No action shall lie under this subsection unless such action is commenced not later than two years after the person adversely affected by a violation described in paragraph (1) first learns, or by which such person reasonably should have learned, of the facts and circumstances giving rise to the action.

SA 2735. Mr. MANCHIN submitted an amendment intended to be proposed to amendment SA 2716 proposed by Mr. BURR (for himself and Mrs. FEINSTEIN) to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 9, between lines 11 and 12, insert the following:

(16) REAL TIME; REAL-TIME.—The terms ''real time'' and ''real-time'' means as close to real time as practicable.

(17) DELAY.—The term ''delay'', with respect to the sharing of a cyber threat indicator, excludes any time necessary to ensure that the cyber threat indicator shared does not contain any personally identifiable information not needed to describe or identify a cybersecurity threat.

(18) MODIFICATION.—The term ''modification'', with respect to the sharing of a cyber threat indicator, excludes any process necessary to ensure that the cyber threat indicator modified does not contain any personally identifiable information not needed to describe or identify a cybersecurity threat.

SA 2736. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ___. PROHIBITION ON THE INDEFINITE DETENTION OF PERSONS BY THE UNITED STATES.

(a) LIMITATION ON DETENTION.—Section 4001 of title 18, United States Code, is amended—

(1) by striking subsection (a) and inserting the following:

''(a) No person shall be imprisoned or otherwise detained by the United States except consistent with the Constitution.'';

(2) by redesignating subsection (b) as subsection (c); and

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

''(b)(1) A general authorization to use military force, a declaration of war, or any similar authority, on its own, shall not be construed to authorize the imprisonment or detention without charge or trial of a person apprehended in the United States.

''(2) Paragraph (1) applies to an authorization to use military force, a declaration of war, or any similar authority enacted before, on, or after the date of the enactment of the Cybersecurity Information Sharing Act of 2015.

''(3) This section shall not be construed to authorize the imprisonment or detention of any person who is apprehended in the United States.''.

(b) REPEAL OF AUTHORITY OF THE ARMED FORCES OF THE UNITED STATES TO DETAIN COVERED PERSONS PURSUANT TO THE AUTHORIZATION FOR USE OF MILITARY FORCE.—Section 1021 of the National Defense Authorization Act for Fiscal Year 2012 (Public Law 112–81; 10 U.S.C. 801 note) is repealed.

SA 2737. Mr. MANCHIN submitted an amendment intended to be proposed to amendment SA 2716 proposed by Mr. BURR (for himself and Mrs. FEINSTEIN) to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 16, strike lines 4 through 10, and insert the following:

(1) IN GENERAL.—

(A) AUTHORIZATION.—Except as provided in subparagraph (B) and paragraph (2) and notwithstanding any other provision of law, an entity may, for the purposes permitted under this Act and consistent with the protection of classified information, share with, or receive from, any other entity or the Federal Government a cyber threat indicator or defensive measure.

(B) EXCEPTION FOR DEPARTMENT OF DEFENSE.—Notwithstanding subparagraph (A), no entity is permitted under this Act to share with the Department of Defense or any component of the Department, including the National Security Agency, a cyber threat indicator or defensive measure.

SA 2738. Mr. BOOKER (for himself and Mr. HELLER) submitted an amendment intended to be proposed to amendment SA 2716 proposed by Mr. BURR (for himself and Mrs. FEINSTEIN) to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 32, between lines 20 and 21, insert the following:

(6) LIMITATION ON RECEIPT OF CYBER THREAT INDICATORS.—A Federal entity may not receive a cyber threat indicator that another Federal entity shared through the process developed and implemented under paragraph (1) unless the Inspector General of the receiving Federal entity certifies that the receiving Federal entity meets the data security standard for receiving such a cyber threat indicator, as established by the Secretary of Homeland Security.

On page 52, strike line 14 and insert the following:

SEC. 10. REPORT ON REDUCTION OF CYBERSECURITY RISK IN AGENCY DATA CENTERS.

Not later than 1 year after the date of enactment of this Act, the Secretary of Homeland Security, in coordination with the Director of the Office of Management and Budget, shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the feasibility of Federal civilian agencies creating an environment for the reduction in cybersecurity risks in agency data centers, including by—

(1) increasing compartmentalization between systems; and

(2) providing a mix of security controls between such compartments.

SEC. 11. CONFORMING AMENDMENT.

SA 2739. Mr. REED submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ___. CYBERSECURITY TRANSPARENCY.

(a) DEFINITIONS.—In this section—

(1) the term ''Commission'' means the Securities and Exchange Commission;

(2) the term ''issuer'' has the meaning given the term in section 3 of the Securities Exchange Act of 1934 (15 U.S.C. 78c); and

(3) the term ''reporting company'' means any company that is an issuer—

(A) the securities of which are registered under section 12 of the Securities Exchange Act of 1934 (15 U.S.C. 78l); or

(B) that is required to file reports under section 15(d) of such Act (15 U.S.C. 78o(d)).

(b) REQUIREMENT TO ISSUE RULES.—Not later than 360 days after the date of enactment of this Act, the Commission shall issue final rules to require each reporting company, in the annual report submitted under section 13 or section 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m and 78o(d)) or the annual proxy statement submitted under section 14(a) of such Act (15 U.S.C. 78n(a))—

(1) to disclose whether any member of the governing body, such as the board of directors or general partner, of the reporting company is a cybersecurity expert (based on minimum standards established by the Commission, in consultation with the Department of Homeland Security and the National

Institute of Standards and Technology), in such detail as necessary to fully describe the nature of the expertise; and

(2) if no member of the governing body of the reporting company is a cybersecurity expert, to briefly describe how the absence of such expertise was taken into account by such persons responsible for identifying and evaluating nominees for any member of the governing body, such as a nominating committee.

(c) CONSIDERATIONS.—In establishing the minimum standards for a cybersecurity expert for purposes of subsection (b), the Commission, in consultation with the Department of Homeland Security and the National Institute of Standards and Technology, shall consider whether a person has substantive experience with preventing and addressing cybersecurity threats.

SA 2740. Mr. SULLIVAN submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ___. COST-BENEFIT ANALYSIS FOR SMALL BUSINESSES.

Not later than 90 days after the date of enactment of this Act, the Administrator of the Small Business Administration shall—

(1) conduct a cost-benefit analysis for small business concerns (as defined in section 3 of the Small Business Act (15 U.S.C. 632)) adopting measures for the sharing of cyber threat indicators and information related to cybersecurity threats; and

(2) submit to Congress a report detailing the results of the cost-benefit analysis conducted under paragraph (1).

SA 2741. Mr. SULLIVAN submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. DEVELOPMENT OF COMPREHENSIVE STRATEGY ON IMPROVING THE CYBERSECURITY OF THE UNITED STATES.

Not later than 120 days after the date of the enactment of this Act, the Secretary of Commerce, acting through the Under Secretary for Industry and Security, shall submit to Congress a comprehensive strategy for improving the cybersecurity of the United States.

SA 2742. Mr. CARPER submitted an amendment intended to be proposed to amendment SA 2716 proposed by Mr. BURR (for himself and Mrs. FEINSTEIN) to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 76, line 22, insert ''the Director of the Office of Management and Budget and'' before ''the Director of National Intelligence''.

On page 77, line 14, insert ''the Director of the Office of Management and Budget and'' before ''the Director of National Intelligence''.

On page 78, between lines 2 and 3, insert the following:

(d) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to designate an information system as a national security system.

On page 78, line 18, strike ''owned'' and insert ''used''.

Beginning on page 80, line 25, strike ''use'' and all that follows through ''other'' on page 81, line 6, and insert ''intrusion detection and prevention capabilities under section 230(b)(1) of the Homeland Security Act of 2002 for the purpose of ensuring the security of''.

SA 2743. Mr. BURR submitted an amendment intended to be proposed to amendment SA 2716 proposed by Mr. BURR (for himself and Mrs. FEINSTEIN) to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

Beginning on page 113, strike line 1 and all that follows through page 114, line 6.

SA 2744. Mr. LEAHY (for himself and Mr. GRASSLEY) submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the end, add the following:

SEC. 408. GAO REPORT ON CELL-SITE SIMULATORS.

(a) DEFINITION.—In this section, the term ''appropriate congressional committees'' means—

(1) the Committee on the Judiciary and the Committee on Homeland Security and Governmental Affairs of the Senate; and

(2) the Committee on the Judiciary and the Committee on Homeland Security of the House of Representatives.

(b) REPORT.—Not later than September 30, 2017, the Comptroller General of the United States shall submit to the appropriate congressional committees a report regarding the use of cell-site simulators (commonly known as ''IMSI catchers'') by Federal, State, and local agencies inside the United States, which shall include to the extent that information is available—

(1) a list of each Federal, State, and local agency that uses cell-site simulators, and for what purposes;

(2) an explanation of the approval process that Federal, State, and local agencies require prior to use of cell-site simulators, including whether such agencies have written policies;

(3) the number of State and local agencies that are subject to non-disclosure agreements with respect to the use of cell-site simulators, and an analysis of whether the non-disclosure agreements are necessary in light of publicly available information about government use of the devices;

(4) the extent to which the Federal Government is providing or funding the purchase of cell-site simulators for State and local agencies, including which Federal grants are used for such purpose;

(5) an explanation of whether Federal, State, and local agencies obtain judicial approval prior to deployment of cell-site simulators, and if so, what type and with what frequency;

(6) an examination of whether court applications seeking approval for the use of cell-site simulators sufficiently explain how the devices work, including—

(A) whether the devices collect information about non-target phones;

(B) the extent to which the devices disrupt service to non-target phones; and

(C) how each Federal, State, or local agency intends to address deletion of data not associated with the target phone;

(7) whether any Federal, State, or local agencies are using cell-site simulators to obtain the contents of communications or for purposes other than locating a particular cellular device;

(8) whether Federal, State, or local agencies have policies or procedures governing the deletion of information collected by cell-site simulators;

(9) an evaluation of whether Federal, State, or local agencies have adequate training and auditing mechanisms in place regarding the use of cell-site simulators;

(10) an evaluation of compliance by the Department of Justice its components with Department of Justice policy guidance governing the use of cell-site simulator technology; and

(11) an evaluation of compliance by the Department of Homeland Security and its components with Department of Homeland Security policy guidance governing the use of cell-site simulator technology.

SA 2745. Mr. FRANKEN (for himself and Mr. LEAHY) submitted an amendment intended to be proposed to amendment SA 2716 proposed by Mr. BURR (for himself and Mrs. FEINSTEIN) to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

Beginning on page 14, strike line 4 and all that follows through page 39, line 21, and insert the following:

(b) AUTHORIZATION FOR OPERATION OF DEFENSIVE MEASURES.—

(1) IN GENERAL.—Notwithstanding any other provision of law, a private entity may, for cybersecurity purposes, operate a defensive measure that is applied to—

(A) an information system of such private entity in order to protect the rights or property of the private entity;

(B) an information system of another entity upon written consent of such entity for operation of such defensive measure to protect the rights or property of such entity; and

(C) an information system of a Federal entity upon written consent of an authorized representative of such Federal entity for operation of such defensive measure to protect the rights or property of the Federal Government.

(2) CONSTRUCTION.—Nothing in this subsection shall be construed—

(A) to authorize the use of a defensive measure other than as provided in this subsection; or

(B) to limit otherwise lawful activity.

(c) AUTHORIZATION FOR SHARING OR RECEIVING CYBER THREAT INDICATORS OR DEFENSIVE MEASURES.—

(1) IN GENERAL.—Except as provided in paragraph (2) and notwithstanding any other provision of law, an entity may, for a cybersecurity purpose and consistent with the protection of classified information, share with, or receive from, any other entity or the Federal Government a cyber threat indicator or defensive measure.

(2) LAWFUL RESTRICTION.—An entity receiving a cyber threat indicator or defensive measure from another entity or Federal entity shall comply with otherwise lawful restrictions placed on the sharing or use of such cyber threat indicator or defensive measure by the sharing entity or Federal entity.

(3) CONSTRUCTION.—Nothing in this subsection shall be construed—

(A) to authorize the sharing or receiving of a cyber threat indicator or defensive measure other than as provided in this subsection; or

(B) to limit otherwise lawful activity.

(d) PROTECTION AND USE OF INFORMATION.—

(1) SECURITY OF INFORMATION.—An entity operating a defensive measure or providing or receiving a cyber threat indicator or defensive measure under this section shall implement and utilize a security control to protect against unauthorized access to or acquisition of such cyber threat indicator or defensive measure.

(2) REMOVAL OF CERTAIN PERSONAL INFORMATION.—An entity sharing a cyber threat indicator pursuant to this title shall, prior to such sharing—

(A) review such cyber threat indicator to assess whether such cyber threat indicator contains any information that the entity knows at the time of sharing to be personal information or information that identifies a specific person not directly related to a cybersecurity threat and remove such information; or

(B) implement and utilize a technical capability configured to remove any information contained within such indicator that the entity knows at the time of sharing to be personal information or information that identifies a specific person not directly related to a cybersecurity threat.

(3) USE OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES BY ENTITIES.—

(A) IN GENERAL.—Consistent with this title, a cyber threat indicator or defensive measure shared or received under this section may, for cybersecurity purposes—

(i) be used by an entity to operate a defensive measure that is applied to—

(I) an information system of the entity; or

(II) an information system of another entity or a Federal entity upon the written consent of that other entity or that Federal entity; and

(ii) be otherwise used, retained, and further shared by an entity subject to—

(I) an otherwise lawful restriction placed by the sharing entity or Federal entity on such cyber threat indicator or defensive measure; or

(II) an otherwise applicable provision of law.

(B) CONSTRUCTION.—Nothing in this paragraph shall be construed to authorize the use of a cyber threat indicator or defensive measure other than as provided in this section.

(4) USE OF CYBER THREAT INDICATORS BY STATE, TRIBAL, OR LOCAL GOVERNMENT.—

(A) LAW ENFORCEMENT USE.—

(i) PRIOR WRITTEN CONSENT.—Except as provided in clause (ii), a cyber threat indicator shared with a State, tribal, or local government under this section may, with the prior written consent of the entity sharing such indicator, be used by a State, tribal, or local government for the purpose of preventing, investigating, or prosecuting any of the offenses described in section 105(d)(5)(A)(vi).

(ii) ORAL CONSENT.—If exigent circumstances prevent obtaining written consent under clause (i), such consent may be provided orally with subsequent documentation of the consent.

(B) EXEMPTION FROM DISCLOSURE.—A cyber threat indicator shared with a State, tribal, or local government under this section shall be—

(i) deemed voluntarily shared information; and

(ii) exempt from disclosure under any State, tribal, or local law requiring disclosure of information or records.

(C) STATE, TRIBAL, AND LOCAL REGULATORY AUTHORITY.—

(i) IN GENERAL.—Except as provided in clause (ii), a cyber threat indicator or defensive measure shared with a State, tribal, or local government under this title shall not be directly used by any State, tribal, or local government to regulate, including an enforcement action, the lawful activity of any entity, including an activity relating to operating a defensive measure or sharing of a cyber threat indicator.

(ii) REGULATORY AUTHORITY SPECIFICALLY RELATING TO PREVENTION OR MITIGATION OF CYBERSECURITY THREATS.—A cyber threat indicator or defensive measures shared as described in clause (i) may, consistent with a State, tribal, or local government regulatory authority specifically relating to the prevention or mitigation of cybersecurity threats to information systems, inform the development or implementation of a regulation relating to such information systems.

(e) ANTITRUST EXEMPTION.—

(1) IN GENERAL.—Except as provided in section 108(e), it shall not be considered a violation of any provision of antitrust laws for 2 or more private entities to exchange or provide a cyber threat indicator, or assistance relating to the prevention, investigation, or mitigation of a cybersecurity threat, for cybersecurity purposes under this title.

(2) APPLICABILITY.—Paragraph (1) shall apply only to information that is exchanged or assistance provided in order to assist with—

(A) facilitating the prevention, investigation, or mitigation of a cybersecurity threat to an information system or information that is stored on, processed by, or transiting an information system; or

(B) communicating or disclosing a cyber threat indicator to help prevent, investigate, or mitigate the effect of a cybersecurity threat to an information system or information that is stored on, processed by, or transiting an information system.

(f) NO RIGHT OR BENEFIT.—The sharing of a cyber threat indicator with an entity under this title shall not create a right or benefit to similar information by such entity or any other entity.

SEC. 105. SHARING OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES WITH THE FEDERAL GOVERNMENT.

(a) REQUIREMENT FOR POLICIES AND PROCEDURES.—

(1) INTERIM POLICIES AND PROCEDURES.—Not later than 60 days after the date of the enactment of this Act, the Attorney General and the Secretary of Homeland Security shall, in coordination with the heads of the appropriate Federal entities, develop and submit to Congress interim policies and procedures relating to the receipt of cyber threat indicators and defensive measures by the Federal Government.

(2) FINAL POLICIES AND PROCEDURES.—Not later than 180 days after the date of the enactment of this Act, the Attorney General and the Secretary of Homeland Security shall, in coordination with the heads of the appropriate Federal entities, promulgate final policies and procedures relating to the receipt of cyber threat indicators and defensive measures by the Federal Government.

(3) REQUIREMENTS CONCERNING POLICIES AND PROCEDURES.—Consistent with the guidelines required by subsection (b), the policies and procedures developed and promulgated under this subsection shall—

(A) ensure that cyber threat indicators shared with the Federal Government by any entity pursuant to section 104(c) through the real-time process described in subsection (c) of this section—

(i) are shared in an automated manner with all of the appropriate Federal entities;

(ii) are only subject to a delay, modification, or other action due to controls established for such real-time process that could impede real-time receipt by all of the appropriate Federal entities when the delay, modification, or other action is due to controls—

(I) agreed upon unanimously by all of the heads of the appropriate Federal entities;

(II) carried out before any of the appropriate Federal entities retains or uses the cyber threat indicators or defensive measures; and

(III) uniformly applied such that each of the appropriate Federal entities is subject to the same delay, modification, or other action; and

(iii) may be provided to other Federal entities;

(B) ensure that cyber threat indicators shared with the Federal Government by any entity pursuant to section 104 in a manner other than the real time process described in subsection (c) of this section—

(i) are shared as quickly as operationally practicable with all of the appropriate Federal entities;

(ii) are not subject to any unnecessary delay, interference, or any other action that could impede receipt by all of the appropriate Federal entities; and

(iii) may be provided to other Federal entities;

(C) consistent with this title, any other applicable provisions of law, and the fair information practice principles set forth in appendix A of the document entitled ''National Strategy for Trusted Identities in Cyberspace'' and published by the President in April, 2011, govern the retention, use, and dissemination by the Federal Government of cyber threat indicators shared with the Federal Government under this title, including the extent, if any, to which such cyber threat indicators may be used by the Federal Government; and

(D) ensure there are—

(i) audit capabilities; and

(ii) appropriate sanctions in place for officers, employees, or agents of a Federal entity who knowingly and willfully conduct activities under this title in an unauthorized manner.

(4) GUIDELINES FOR ENTITIES SHARING CYBER THREAT INDICATORS WITH FEDERAL GOVERNMENT.—

(A) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, the Attorney General and the Secretary of Homeland Security shall develop and make publicly available guidance to assist entities and promote sharing of cyber threat indicators with Federal entities under this title.

(B) CONTENTS.—The guidelines developed and made publicly available under subparagraph (A) shall include guidance on the following:

(i) Identification of types of information that would qualify as a cyber threat indicator under this title that would be unlikely to include personal information or information that identifies a specific person not directly related to a cyber security threat.

(ii) Identification of types of information protected under otherwise applicable privacy laws that are unlikely to be directly related to a cybersecurity threat.

(iii) Such other matters as the Attorney General and the Secretary of Homeland Security consider appropriate for entities sharing cyber threat indicators with Federal entities under this title.

(b) PRIVACY AND CIVIL LIBERTIES.—

(1) GUIDELINES OF ATTORNEY GENERAL.—Not later than 60 days after the date of the enactment of this Act, the Attorney General shall, in coordination with heads of the appropriate Federal entities and in consultation with officers designated under section 1062 of the National Security Intelligence Reform Act of 2004 (42 U.S.C. 2000ee–1), develop, submit to Congress, and make available to the public interim guidelines relating to privacy and civil liberties which shall govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in connection with activities authorized in this title.

(2) FINAL GUIDELINES.—

(A) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Attorney General shall, in coordination with heads of the appropriate Federal entities and in consultation with officers designated under section 1062 of the National Security Intelligence Reform Act of 2004 (42 U.S.C. 2000ee–1) and such private entities with industry expertise as the Attorney General considers relevant, promulgate final guidelines relating to privacy and civil liberties which shall govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in connection with activities authorized in this title.

(B) PERIODIC REVIEW.—The Attorney General shall, in coordination with heads of the appropriate Federal entities and in consultation with officers and private entities described in subparagraph (A), periodically, but not less frequently than once every two years, review the guidelines promulgated under subparagraph (A).

(3) CONTENT.—The guidelines required by paragraphs (1) and (2) shall, consistent with the need to protect information systems from cybersecurity threats and mitigate cybersecurity threats—

(A) limit the effect on privacy and civil liberties of activities by the Federal Government under this title;

(B) limit the receipt, retention, use, and dissemination of cyber threat indicators containing personal information or information that identifies specific persons, including by establishing—

(i) a process for the timely destruction of such information that is known not to be directly related to uses authorized under this title; and

(ii) specific limitations on the length of any period in which a cyber threat indicator may be retained;

(C) include requirements to safeguard cyber threat indicators containing personal information or information that identifies specific persons from unauthorized access or acquisition, including appropriate sanctions for activities by officers, employees, or agents of the Federal Government in contravention of such guidelines;

(D) include procedures for notifying entities and Federal entities if information received pursuant to this section is known or determined by a Federal entity receiving such information not to constitute a cyber threat indicator;

(E) protect the confidentiality of cyber threat indicators containing personal information or information that identifies specific persons to the greatest extent practicable and require recipients to be informed that such indicators may only be used for purposes authorized under this title; and

(F) include steps that may be needed so that dissemination of cyber threat indicators is consistent with the protection of classified and other sensitive national security information.

(c) CAPABILITY AND PROCESS WITHIN THE DEPARTMENT OF HOMELAND SECURITY.—

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Secretary of Homeland Security, in coordination with the heads of the appropriate Federal entities, shall develop and implement a capability and process within the Department of Homeland Security that—

(A) shall accept from any entity in real time cyber threat indicators and defensive measures, pursuant to this section;

(B) shall, upon submittal of the certification under paragraph (2) that such capability and process fully and effectively operates as described in such paragraph, be the process by which the Federal Government receives cyber threat indicators and defensive measures under this title that are shared by a private entity with the Federal Government through electronic mail or media, an interactive form on an Internet website, or a real time, automated process between information systems except—

(i) consistent with section 104, communications between a Federal entity and a private entity regarding a previously shared cyber threat indicator to describe the relevant cybersecurity threat or develop a defensive measure based on such cyber threat indicator; and

(ii) communications by a regulated entity with such entity's Federal regulatory authority regarding a cybersecurity threat;

(C) ensures that all of the appropriate Federal entities receive in an automated manner such cyber threat indicators shared through the real-time process within the Department of Homeland Security;

(D) is in compliance with the policies, procedures, and guidelines required by this section; and

(E) does not limit or prohibit otherwise lawful disclosures of communications, records, or other information, including—

(i) reporting of known or suspected criminal activity, by an entity to any other entity or a Federal entity;

(ii) voluntary or legally compelled participation in a Federal investigation; and

(iii) providing cyber threat indicators or defensive measures as part of a statutory or authorized contractual requirement.

(2) CERTIFICATION.—Not later than 10 days prior to the implementation of the capability and process required by paragraph (1), the Secretary of Homeland Security shall, in consultation with the heads of the appropriate Federal entities, certify to Congress whether such capability and process fully and effectively operates—

(A) as the process by which the Federal Government receives from any entity a cyber threat indicator or defensive measure under this title; and

(B) in accordance with the policies, procedures, and guidelines developed under this section.

(3) PUBLIC NOTICE AND ACCESS.—The Secretary of Homeland Security shall ensure there is public notice of, and access to, the capability and process developed and implemented under paragraph (1) so that—

(A) any entity may share cyber threat indicators and defensive measures through such process with the Federal Government; and

(B) all of the appropriate Federal entities receive such cyber threat indicators and defensive measures in real time with receipt through the process within the Department of Homeland Security.

(4) OTHER FEDERAL ENTITIES.—The process developed and implemented under paragraph (1) shall ensure that other Federal entities receive in a timely manner any cyber threat indicators and defensive measures shared with the Federal Government through such process.

(5) REPORT ON DEVELOPMENT AND IMPLEMENTATION.—

(A) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to Congress a report on the development and implementation of the capability and process required by paragraph (1), including a description of such capability and process and the public notice of, and access to, such process.

(B) CLASSIFIED ANNEX.—The report required by subparagraph (A) shall be submitted in unclassified form, but may include a classified annex.

(d) INFORMATION SHARED WITH OR PROVIDED TO THE FEDERAL GOVERNMENT.—

(1) NO WAIVER OF PRIVILEGE OR PROTECTION.—The provision of cyber threat indicators and defensive measures to the Federal Government under this title shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection.

(2) PROPRIETARY INFORMATION.—Consistent with section 104(c)(2), a cyber threat indicator or defensive measure provided by an entity to the Federal Government under this title shall be considered the commercial, financial, and proprietary information of such entity when so designated by the originating entity or a third party acting in accordance with the written authorization of the originating entity.

(3) EXEMPTION FROM DISCLOSURE.—Cyber threat indicators and defensive measures provided to the Federal Government under this title shall be—

(A) deemed voluntarily shared information and exempt from disclosure under section 552 of title 5, United States Code, and any State, tribal, or local law requiring disclosure of information or records; and

(B) withheld, without discretion, from the public under section 552(b)(3)(B) of title 5, United States Code, and any State, tribal, or local provision of law requiring disclosure of information or records.

(4) EX PARTE COMMUNICATIONS.—The provision of a cyber threat indicator or defensive measure to the Federal Government under this title shall not be subject to a rule of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official.

(5) DISCLOSURE, RETENTION, AND USE.—

(A) AUTHORIZED ACTIVITIES.—Cyber threat indicators and defensive measures provided to the Federal Government under this title may be disclosed to, retained by, and used by, consistent with otherwise applicable provisions of Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal Government solely for—

(i) a cybersecurity purpose;

(ii) the purpose of identifying a cybersecurity threat, including the source of such cybersecurity threat, or a security vulnerability;

(iii) the purpose of identifying a cybersecurity threat involving the use of an information system by a foreign adversary or terrorist;

(iv) the purpose of responding to, or otherwise preventing or mitigating, an imminent threat of death, serious bodily harm, or serious economic harm, including a terrorist act or a use of a weapon of mass destruction;

(v) the purpose of responding to, or otherwise preventing or mitigating, a serious threat to a minor, including sexual exploitation and threats to physical safety; or

(vi) the purpose of preventing, investigating, disrupting, or prosecuting an offense arising out of a threat described in clause (iv) or any of the offenses listed in—

(I) sections 1028 through 1030 of title 18, United States Code (relating to fraud and identity theft);

(II) chapter 37 of such title (relating to espionage and censorship); and

(III) chapter 90 of such title (relating to protection of trade secrets).

(B) PROHIBITED ACTIVITIES.—Cyber threat indicators and defensive measures provided to the Federal Government under this title shall not be disclosed to, retained by, or used by any Federal agency or department for any use not permitted under subparagraph (A).

(C) PRIVACY AND CIVIL LIBERTIES.—Cyber threat indicators and defensive measures provided to the Federal Government under this title shall be retained, used, and disseminated by the Federal Government—

(i) in accordance with the policies, procedures, and guidelines required by subsections (a) and (b);

(ii) in a manner that protects from unauthorized use or disclosure any cyber threat indicators that may contain personal information or information that identifies specific persons; and

(iii) in a manner that protects the confidentiality of cyber threat indicators containing personal information or information that identifies a specific person.

(D) FEDERAL REGULATORY AUTHORITY.—

(i) IN GENERAL.—Except as provided in clause (ii), cyber threat indicators and defensive measures provided to the Federal Government under this title shall not be directly used by any Federal, State, tribal, or local government to regulate, including an enforcement action, the lawful activities of any entity, including activities relating to operating defensive measures or sharing cyber threat indicators.

(ii) EXCEPTIONS.—

(I) REGULATORY AUTHORITY SPECIFICALLY RELATING TO PREVENTION OR MITIGATION OF CYBERSECURITY THREATS.—Cyber threat indicators and defensive measures provided to the Federal Government under this title may, consistent with Federal or State regulatory authority specifically relating to the prevention or mitigation of cybersecurity threats to information systems, inform the development or implementation of regulations relating to such information systems.

(II) PROCEDURES DEVELOPED AND IMPLEMENTED UNDER THIS TITLE.—Clause (i) shall not apply to procedures developed and implemented under this title.

SEC. 106. PROTECTION FROM LIABILITY.

SA 2746. Mr. BURR submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 11, line 3, strike ''period'' and insert ''periodic''.

On page 20, line 21, strike ''measures'' and insert ''measure''.

On page 56, line 8, strike ''and'' and all that follows through ''(7)'' on line 9 and insert the following:

(7) the term ''national security system'' has the meaning given the term in section 11103 of title 40, United States Code; and

(8)

On page 57, line 8, strike ''and''.

On page 57, line 11, strike the period at the end and insert ''; and''.

On page 57, between lines 11 and 12, insert the following:

''(4) the term 'national security system' has the meaning given the term in section 11103 of title 40, United States Code.

On page 64, lines 14 and 15, strike ''Notwithstanding section 202, in this subsection'' and insert ''In this subsection only''.

On page 69, line 13, strike ''all taken'' and insert ''taken all''.

On page 76, line 22, insert ''and the Director of the Office of Management and Budget'' after ''Intelligence''.

On page 77, lines 12 and 13, strike '', as defined in section 11103 of title 40, United States Code''.

On page 77, line 14, insert ''and the Director of the Office of Management and Budget'' after ''Intelligence''.

On page 78, between lines 2 and 3, insert the following:

(d) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to designate an information system as a national security system.

On page 78, line 18, strike ''owned'' and insert ''used''.

Beginning on page 80, line 25, strike ''use'' and all that follows through ''other'' on page 81, line 6, and insert ''intrusion detection and prevention capabilities under section 230(b)(1) of the Homeland Security Act of 2002 for the purpose of ensuring the security of''.

On page 84, line 25, strike ''Act'' and insert ''Act of 2015''.

On page 88, line 8, strike ''non-civilian'' and insert ''noncivilian''.

On page 91, line 11, strike ''203 and 204'' and insert ''303 and 304''.

On page 96, line 19, strike ''likely,'' and insert ''likely''.

On page 96, line 22, strike ''present'' and insert ''present,''.

On page 107, line 10, strike ''shall each'' and insert ''shall''.

On page 107, lines 11 and 12, strike ''each Comptroller General of the United States and''.

On page 110, strikes lines 6 through 16.

On page 114, line 7, strike ''SENATE'' and insert ''SENSE''.

SA 2747. Mr. VITTER proposed an amendment to the bill H.R. 208, to improve the disaster assistance programs of the Small Business Administration; as follows:

On page 2, strike lines 1 through 5 and insert the following:

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Recovery Improvements for Small Entities After Disaster Act of 2015'' or the ''RISE After Disaster Act of 2015''.

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

DIVISION A—SUPERSTORM SANDY RELIEF AND DISASTER LOAN PROGRAM IMPROVEMENTS

SEC. 1001. SHORT TITLE.

This division may be cited as the ''Superstorm Sandy Relief and Disaster Loan Program Improvement Act of 2015''.

SEC. 1002. FINDINGS.

On page 3, strike line 5 and insert the following:

TITLE I—DISASTER ASSISTANCE IMPROVEMENTS

SEC. 1101. REVISED DISASTER DEADLINE.

On page 3, line 14, insert ''nonprofit entity,'' after ''homeowner,''.

On page 4, line 9, strike the quotation marks and the second period and insert the following:

''(C) INSPECTOR GENERAL REVIEW.—Not later than 6 months after the date on which the Administrator begins carrying out this authority, the Inspector General of the Administration shall initiate a review of the controls for ensuring applicant eligibility for loans made under this paragraph.''.

On page 4, line 10, strike ''**SEC. 4.**'' and insert ''**SEC. 1102.**''.

On page 4, line 24, insert '', if such safe room or similar storm shelter is constructed in accordance with applicable standards issued by the Federal Emergency Management Agency'' after ''disasters''.

On page 5, strike lines 1 through 21 and insert the following:

SEC. 1103. REDUCING DELAYS ON CLOSING AND DISBURSEMENT OF LOANS.

Section 7(b) of the Small Business Act (15 U.S.C. 636(b)) is amended by inserting before the undesignated matter following paragraph (9) the following:

On page 5, line 22, strike ''(11)'' and insert ''(10)''.

On page 6, strike lines 5 through 8 and insert the following:

SEC. 1104. SAFEGUARDING TAXPAYER INTERESTS AND INCREASING TRANSPARENCY IN LOAN APPROVALS.

Section 7(b) of the Small Business Act (15 U.S.C. 636(b)) is amended by inserting before the undesignated matter following paragraph (10), as added by section 1103 of this Act, the following:

On page 6, line 9, strike ''(12)'' and insert ''(11)''.

Beginning on page 6, strike line 14 and all that follows through page 7, line 20, and insert the following:

SEC. 1105. DISASTER PLAN IMPROVEMENTS.

Beginning on page 8, strike line 6 and all that follows through page 9, line 6, and insert the following:

DIVISION B—RECOVERY IMPROVEMENTS FOR SMALL ENTITIES

SECTION 2001. SHORT TITLE.

This division may be cited as the ''Recovery Improvements for Small Entities After Disaster Act of 2015'' or the ''RISE After Disaster Act of 2015''.

TITLE I—IMPROVEMENTS OF DISASTER RESPONSE AND LOANS

SEC. 2101. ADDITIONAL AWARDS TO SMALL BUSINESS DEVELOPMENT CENTERS, WOMEN'S BUSINESS CENTERS, AND SCORE FOR DISASTER RECOVERY.

Section 7(b) of the Small Business Act (15 U.S.C. 636(b)) is amended by inserting before the undesignated matter following paragraph (11), as added by section 1104 of this Act, the following:

''(12) ADDITIONAL AWARDS TO SMALL BUSINESS DEVELOPMENT CENTERS, WOMEN'S BUSINESS CENTERS, AND SCORE FOR DISASTER RECOVERY.—

''(A) IN GENERAL.—The Administration may provide financial assistance to a small business development center, a women's business center described in section 29, the Service Corps of Retired Executives, or any proposed consortium of such individuals or entities to spur disaster recovery and growth of small business concerns located in an area for which the President has declared a major disaster.

''(B) FORM OF FINANCIAL ASSISTANCE.—Financial assistance provided under this paragraph shall be in the form of a grant, contract, or cooperative agreement.

''(C) NO MATCHING FUNDS REQUIRED.—Matching funds shall not be required for any grant, contract, or cooperative agreement under this paragraph.

''(D) REQUIREMENTS.—A recipient of financial assistance under this paragraph shall provide counseling, training, and other related services, such as promoting long-term resiliency, to small business concerns and entrepreneurs impacted by a major disaster.

''(E) PERFORMANCE.—

''(i) IN GENERAL.—The Administrator, in cooperation with the recipients of financial assistance under this paragraph, shall establish metrics and goals for performance of grants, contracts, and cooperative agreements under this paragraph, which shall include recovery of sales, recovery of employment, reestablishment of business premises, and establishment of new small business concerns.

''(ii) USE OF ESTIMATES.—The Administrator shall base the goals and metrics for performance established under clause (i), in part, on the estimates of disaster impact prepared by the Office of Disaster Assistance for purposes of estimating loan-making requirements.

''(F) TERM.—

''(i) IN GENERAL.—The term of any grant, contract, or cooperative agreement under this paragraph shall be for not more than 2 years.

''(ii) EXTENSION.—The Administrator may make 1 extension of a grant, contract, or cooperative agreement under this paragraph for a period of not more than 1 year, upon a showing of good cause and need for the extension.

''(G) EXEMPTION FROM OTHER PROGRAM REQUIREMENTS.—Financial assistance provided under this paragraph is in addition to, and wholly separate from, any other form of assistance provided by the Administrator under this Act.

''(H) COMPETITIVE BASIS.—The Administration shall award financial assistance under this paragraph on a competitive basis.''.

SEC. 2102. COLLATERAL REQUIREMENTS FOR DISASTER LOANS.

(a) IN GENERAL.—Section 7(d)(6) of the Small Business Act (15 U.S.C. 636(d)(6)) is amended in the third proviso—

(1) by striking ''$14,000'' and inserting ''$25,000''; and

(2) by striking ''major disaster'' and inserting ''disaster''.

(b) SUNSET.—Effective on the date that is 3 years after the date of enactment of this Act, section 7(d)(6) of the Small Business Act (15 U.S.C. 636(d)(6)) is amended in the third proviso—

(1) by striking ''$25,000'' and inserting ''$14,000''; and

(2) by inserting ''major'' before ''disaster''.

(c) REPORT.—Not later than 180 days before the date on which the amendments made by subsection (b) are to take effect, the Administrator of the Small Business Administration shall submit to Committee on Small Business and Entrepreneurship of the Senate and the Committee on Small Business of the House of Representatives a report on the effects of the amendments made by subsection (a), which shall include—

(1) an assessment of the impact and benefits resulting from the amendments; and

(2) a recommendation as to whether the amendments should be made permanent.

SEC. 2103. ASSISTANCE TO OUT-OF-STATE BUSINESS CONCERNS TO AID IN DISASTER RECOVERY.

(a) IN GENERAL.—Section 21(b)(3) of the Small Business Act (15 U.S.C. 648(b)(3)) is amended—

(1) by striking ''(3) At the discretion'' and inserting the following:

''(3) ASSISTANCE TO OUT-OF-STATE SMALL BUSINESS CONCERNS.—

''(A) IN GENERAL.—At the discretion''; and

(2) by adding at the end the following:

''(B) DISASTER RECOVERY ASSISTANCE.—

''(i) IN GENERAL.—At the discretion of the Administrator, the Administrator may authorize a small business development center to provide advice, information, and assistance, as described in subsection (c), to a small business concern located outside of the State, without regard to geographic proximity to the small business development center, if the small business concern is located in an area for which the President has declared a major disaster.

''(ii) TERM.—

''(I) IN GENERAL.—A small business development center may provide advice, information, and assistance to a small business concern under clause (i) for a period of not more than 2 years after the date on which the President declared a major disaster for the area in which the small business concern is located.

''(II) EXTENSION.—The Administrator may, at the discretion of the Administrator, extend the period described in subclause (I).

''(iii) CONTINUITY OF SERVICES.—A small business development center that provides counselors to an area described in clause (i) shall, to the maximum extent practicable, ensure continuity of services in any State in which the small business development center otherwise provides services.

''(iv) ACCESS TO DISASTER RECOVERY FACILITIES.—For purposes of this subparagraph, the Administrator shall, to the maximum extent practicable, permit the personnel of a small business development center to use any site or facility designated by the Administrator for use to provide disaster recovery assistance.''.

(b) SENSE OF CONGRESS.—It is the sense of Congress that, subject to the availability of funds, the Administrator of the Small Business Administration should, to the extent practicable, ensure that a small business development center is appropriately reimbursed for any legitimate expenses incurred in carrying out activities under section 21(b)(3)(B) of the Small Business Act, as added by subsection (a).

SEC. 2105. FAST PROGRAM.

(a) DEFINITIONS.—Section 34(a) of the Small Business Act (15 U.S.C. 657d(a)) is amended—

(1) by redesignating paragraphs (3) through (9) as paragraphs (4) through (10), respectively; and

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

''(3) CATASTROPHIC INCIDENT.—The term 'catastrophic incident' means a major disaster that is comparable to the description of a catastrophic incident in the National Response Plan of the Administration, or any successor thereto.''.

(b) PRIORITY.—Section 34(c)(2) of the Small Business Act (15 U.S.C. 657d(c)(2)) is amended—

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

(2) in subparagraph (B)(vi)(III), by striking the period at the end and inserting ''; and''; and

(3) by adding at the end the following:

''(C) shall give special consideration to an applicant that is located in an area affected by a catastrophic incident.''.

(c) ADDITIONAL ASSISTANCE.—Section 34(c) of the Small Business Act (15 U.S.C. 657d(c)) is amended by adding at the end the following:

''(5) ADDITIONAL ASSISTANCE FOR CATASTROPHIC INCIDENTS.—Upon application by an applicant that receives an award or has in effect a cooperative agreement under this section and that is located in an area affected by a catastrophic incident, the Administrator may—

''(A) provide additional assistance to the applicant; and

''(B) waive the matching requirements under subsection (e)(2).''.

SEC. 2106. USE OF FEDERAL SURPLUS PROPERTY IN DISASTER AREAS.

Section 7(j)(13)(F) of the Small Business Act (15 U.S.C. 636(j)(13)(F)) is amended—

(1) by inserting ''(i)'' after ''(F)''; and

(2) by adding at the end the following:

''(ii)(I) In this clause—

''(aa) the term 'covered period' means the 2-year period beginning on the date on which the President declared the applicable major disaster; and

''(bb) the term 'disaster area' means the area for which the President has declared a major disaster, during the covered period.

''(II) The Administrator may transfer technology or surplus property under clause (i) on a priority basis to a small business concern located in a disaster area if—

''(aa) the small business concern meets the requirements for such a transfer, without regard to whether the small business concern is a Program Participant; and

''(bb) for a small business concern that is a Program Participant, on and after the date on which the President declared the applicable major disaster, the small business concern has not received property under this subparagraph on the basis of the status of the small business concern as a Program Participant.

''(III) For any transfer of property under this clause to a small business concern, the terms and conditions shall be the same as a transfer to a Program Participant, except that the small business concern shall agree not to sell or transfer the property to any party other than the Federal Government during the covered period.

''(IV) A small business concern that receives a transfer of property under this clause may not receive a transfer of property under clause (i) during the covered period.

''(V) If a small business concern sells or transfers property in violation of the agreement described in subclause (III), the Administrator may initiate proceedings to prohibit the small business concern from receiving a transfer of property under this clause or clause (i), in addition to any other remedy available to the Administrator.''.

SEC. 2107. RECOVERY OPPORTUNITY LOANS.

Section 7(a)(31) of the Small Business Act (15 U.S.C. 636(a)(31)) is amended—

(1) in subparagraph (A)—

(A) by redesignating clauses (i), (ii), and (iii) as clauses (ii), (iii), and (iv), respectively; and

(B) by inserting before clause (ii), as so redesignated, the following:

''(i) The term 'disaster area' means the area for which the President has declared a major disaster, during the 5-year period beginning on the date of the declaration.''; and

(2) by adding at the end the following:

''(H) RECOVERY OPPORTUNITY LOANS.—

''(i) IN GENERAL.—The Administrator may guarantee an express loan to a small business concern located in a disaster area in accordance with this subparagraph.

''(ii) MAXIMUMS.—For a loan guaranteed under clause (i)—

''(I) the maximum loan amount is $150,000; and

''(II) the guarantee rate shall be not more than 85 percent.

''(iii) OVERALL CAP.—A loan guaranteed under clause (i) shall not be counted in determining the amount of loans made to a borrower for purposes of subparagraph (D).

''(iv) OPERATIONS.—A small business concern receiving a loan guaranteed under clause (i) shall certify that the small business concern was in operation on the date on which the applicable major disaster occurred as a condition of receiving the loan.

''(v) REPAYMENT ABILITY.—A loan guaranteed under clause (i) may only be made to a small business concern that demonstrates, to the satisfaction of the Administrator, sufficient capacity to repay the loan.

''(vi) TIMING OF PAYMENT OF GUARANTEES.—

''(I) IN GENERAL.—Not later than 90 days after the date on which a request for purchase is filed with the Administrator, the Administrator shall determine whether to pay the guaranteed portion of the loan.

''(II) RECAPTURE.—Notwithstanding any other provision of law, unless there is a subsequent finding of fraud by a court of competent jurisdiction relating to a loan guaranteed under clause (i), on and after the date that is 6 months after the date on which the Administrator determines to pay the guaranteed portion of the loan, the Administrator may not attempt to recapture the paid guarantee.

''(vii) FEES.—

''(I) IN GENERAL.—Unless the Administrator has waived the guarantee fee that would otherwise be collected by the Administrator under paragraph (18) for a loan guaranteed under clause (i), and except as provided in subclause (II), the guarantee fee for the loan shall be equal to the guarantee fee that the Administrator would collect if the guarantee rate for the loan was 50 percent.

''(II) EXCEPTION.—Subclause (I) shall not apply if the cost of carrying out the program under this subsection in a fiscal year is more than zero and such cost is directly attributable to the cost of guaranteeing loans under clause (i).

''(viii) RULES.—Not later than 270 days after the date of enactment of this subparagraph, the Administrator shall promulgate rules to carry out this subparagraph.''.

SEC. 2108. CONTRACTOR MALFEASANCE.

Section 7(b) of the Small Business Act (15 U.S.C. 636(b)) is amended by inserting before the undesignated matter following paragraph (12), as added by section 2101 of this Act, the following:

''(13) SUPPLEMENTAL ASSISTANCE FOR CONTRACTOR MALFEASANCE.—

''(A) IN GENERAL.—If a contractor or other person engages in malfeasance in connection with repairs to, rehabilitation of, or replacement of real or personal property relating to which a loan was made under this subsection and the malfeasance results in substantial economic damage to the recipient of the loan or substantial risks to health or safety, upon receiving documentation of the substantial economic damage or the substantial risk to health and safety from an independent loss verifier, and subject to subparagraph (B), the Administrator may increase the amount of the loan under this subsection, as necessary for the cost of repairs, rehabilitation, or replacement needed to address the cause of the economic damage or health or safety risk.

''(B) REQUIREMENTS.—The Administrator may only increase the amount of a loan under subparagraph (A) upon receiving an appropriate certification from the borrower and person performing the mitigation attesting to the reasonableness of the mitigation costs and an assignment of any proceeds received from the person engaging in the malfeasance. The assignment of proceeds recovered from the person engaging in the malfeasance shall be equal to the amount of the loan under this section. Any mitigation activities shall be subject to audit and independent verification of completeness and cost reasonableness.''.

SEC. 2109. LOCAL CONTRACTING PREFERENCES AND INCENTIVES.

Section 15 of the Small Business Act (15 U.S.C. 644) is amended by inserting after subsection (e) the following:

''(f) CONTRACTING PREFERENCE FOR SMALL BUSINESS CONCERNS IN A MAJOR DISASTER AREA.—

''(1) DEFINITION.—In this subsection, the term 'disaster area' means the area for which the President has declared a major disaster, during the period of the declaration.

''(2) CONTRACTING PREFERENCE.—An agency shall provide a contracting preference for a small business concern located in a disaster area if the small business concern will perform the work required under the contract in the disaster area.

''(3) CREDIT FOR MEETING CONTRACTING GOALS.—If an agency awards a contract to a small business concern under the circumstances described in paragraph (2), the value of the contract shall be doubled for purposes of determining compliance with the goals for procurement contracts under subsection (g)(1)(A).''.

SEC. 2110. CLARIFICATION OF COLLATERAL REQUIREMENTS.

Section 7(d)(6) of the Small Business Act (15 U.S.C. 636(d)(6)) is amended by inserting after ''which are made under paragraph (1) of subsection (b)'' the following: '': *Provided further*, That the Administrator, in obtaining the best available collateral for a loan of not more than $200,000 under paragraph (1) or (2) of subsection (b) relating to damage to or destruction of the property of, or economic injury to, a small business concern, shall not require the owner of the small business concern to use the primary residence of the owner as collateral if the Administrator determines that the owner has other assets of equal quality and with a value equal to or greater than the amount of the loan that could be used as collateral for the loan: *Provided further*, That nothing in the preceding proviso may be construed to reduce the amount of collateral required by the Administrator in connection with a loan described in the preceding proviso or to modify the standards used to evaluate the quality (rather than the type) of such collateral''.

TITLE II—DISASTER PLANNING AND MITIGATION

SEC. 2201. BUSINESS RECOVERY CENTERS.

Section 7(b) of the Small Business Act (15 U.S.C. 636(b)) is amended by inserting before the undesignated matter following paragraph (13), as added by section 2108 of this Act, the following:

''(14) BUSINESS RECOVERY CENTERS.—

''(A) IN GENERAL.—The Administrator, acting through the district offices of the Administration, shall identify locations that may be used as recovery centers by the Administration in the event of a disaster declared under this subsection or a major disaster.

''(B) REQUIREMENTS FOR IDENTIFICATION.—Each district office of the Administration shall—

''(i) identify a location described in subparagraph (A) in each county, parish, or similar unit of general local government in the area served by the district office; and

''(ii) ensure that the locations identified under subparagraph (A) may be used as a recovery center without cost to the Government, to the extent practicable.''.

TITLE III—OTHER PROVISIONS

SEC. 2301. INCREASED OVERSIGHT OF ECONOMIC INJURY DISASTER LOANS.

(a) IN GENERAL.—Section 7(b) of the Small Business Act (15 U.S.C. 636(b)) is amended by inserting before the undesignated matter following paragraph (14), as added by section 2201 of this Act, the following:

''(15) INCREASED OVERSIGHT OF ECONOMIC INJURY DISASTER LOANS.—The Administrator shall increase oversight of entities receiving loans under paragraph (2), and may consider—

''(A) scheduled site visits to ensure borrower eligibility and compliance with requirements established by the Administrator; and

''(B) reviews of the use of the loan proceeds by an entity described in paragraph (2) to ensure compliance with requirements established by the Administrator.''.

(b) SENSE OF CONGRESS RELATING TO USING EXISTING FUNDS.—It is the sense of Congress that no additional Federal funds should be made available to carry out the amendments made by this section.

SEC. 2302. GAO REPORT ON PAPERWORK REDUCTION.

Not later than 1 year after the date of enactment of this Act, the Comptroller General of the United States shall submit to the Committee on Small Business and Entrepreneurship of the Senate and the Committee on Small Business of the House of Representatives a report evaluating steps that the Small Business Administration has taken, with respect to the application for disaster assistance under section 7(b) of the Small Business Act (15 U.S.C. 636(b)), to comply with subchapter I of chapter 35 of title 44, United States Code (commonly known as the ''Paperwork Reduction Act'') and related guidance.

SEC. 2303. REPORT ON WEB PORTAL FOR DISASTER LOAN APPLICANTS.

Section 38 of the Small Business Act (15 U.S.C. 657j) is amended by adding at the end the following:

''(c) REPORT ON WEB PORTAL FOR DISASTER LOAN APPLICATION STATUS.—

''(1) IN GENERAL.—Not later than 90 days after the date of enactment of this subsection, the Administrator shall submit to the Committee on Small Business and Entrepreneurship of the Senate and the Committee on Small Business of the House of

Representatives a report relating to the creation of a web portal to the track the status of applications for disaster assistance under section 7(b).

''(2) CONTENTS.—The report under paragraph (1) shall include—

''(A) information on the progress of the Administration in implementing the information system under subsection (a);

''(B) recommendations from the Administration relating to the creation of a web portal for applicants to check the status of an application for disaster assistance under section 7(b), including a review of best practices and web portal models from the private sector;

''(C) information on any related costs or staffing needed to implement such a web portal;

''(D) information on whether such a web portal can maintain high standards for data privacy and data security;

''(E) information on whether such a web portal will minimize redundancy among Administration disaster programs, improve management of the number of inquiries made by disaster applicants to employees located in the area affected by the disaster and to call centers, and reduce paperwork burdens on disaster victims; and

''(F) such additional information as is determined necessary by the Administrator.''.

AUTHORITY FOR COMMITTEES TO MEET

COMMITTEE ON AGRICULTURE, NUTRITION, AND FORESTRY

Mr. SULLIVAN. Mr. President, I ask unanimous consent that the Committee on Agriculture, Nutrition, and Forestry be authorized to meet during the session of the Senate on October 21, 2015, at 10 a.m. in room SD–106 of the Dirksen Senate Office Building, to conduct a hearing entitled ''Agriculture Biotechnology: A Look at Federal Regulation and Stakeholder Perspectives.''

The PRESIDING OFFICER. Without objection, it is so ordered.

COMMITTEE ON ARMED SERVICES

Mr. SULLIVAN. Mr. President, I ask unanimous consent that the Committee on Armed Services be authorized to meet during the session of the Senate on October 21, 2015, at 9:30 a.m.

The PRESIDING OFFICER. Without objection, it is so ordered.

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

Mr. SULLIVAN. Mr. President, I ask unanimous consent that the Committee on Homeland Security and Governmental Affairs be authorized to meet during the session of the Senate on October 21, 2015, at 9:30 a.m. to conduct a hearing entitled ''Ongoing Migration from Central America: An Examination of FY2015 Apprehensions.''

The PRESIDING OFFICER. Without objection, it is so ordered.

COMMITTEE ON INDIAN AFFAIRS

Mr. SULLIVAN. Mr. President, I ask unanimous consent that the Committee on Indian Affairs be authorized to meet during the session of the Senate on October 21, 2015, at 2:15 p.m., in room SD–628 of the Dirksen Senate Office Building, to conduct a hearing entitled ''The GAO Report on 'INDIAN ENERGY DEVELOPMENT: Poor Management by BIA Has Hindered Development on Indian Lands.' ''

The PRESIDING OFFICER. Without objection, it is so ordered.

COMMITTEE ON THE JUDICIARY

Mr. SULLIVAN. Mr. President, I ask unanimous consent that the Committee on the Judiciary be authorized to meet during the session of the Senate on October 21, 2015, at 10 a.m., in room SD–226 of the Dirksen Senate Office Building, to conduct a hearing entitled ''Nominations.''

The PRESIDING OFFICER. Without objection, it is so ordered.

SPECIAL COMMITTEE ON AGING

Mr. SULLIVAN. Mr. President, I ask unanimous consent that the Special Committee on Aging be authorized to meet during the session of the Senate on October 21, 2015, at 2:30 p.m., in room SD–562 of the Dirksen Senate Office Building, to conduct a hearing entitled ''Virtual Victims: When Computer Tech Support Becomes a Scam.''

The PRESIDING OFFICER. Without objection, it is so ordered.

SUBCOMMITTEE ON SUPERFUND, WASTE MANAGEMENT, AND REGULATORY OVERSIGHT

Mr. SULLIVAN. Mr. President, I ask unanimous consent that the Subcommittee on Superfund, Waste Management, and Regulatory Oversight of the Committee on Environment and Public Works be authorized to meet during the session of the Senate on October 21, 2015, at 10 a.m., in room SD–406 of the Dirksen Senate Office Building, to conduct a hearing entitled ''Oversight of Regulatory Impact Analyses for U.S. Environmental Protection Agency Regulations.''

The PRESIDING OFFICER. Without objection, it is so ordered.

HONORING THE LIVES OF THE 33 CREW MEMBERS ABOARD THE ''EL FARO''

Mr. MCCONNELL. Mr. President, I ask unanimous consent that the Senate proceed to the consideration of S. Res. 291, submitted earlier today.

The PRESIDING OFFICER. The clerk will report the resolution by title.

The bill clerk read as follows:

A resolution (S. Res. 291) honoring the lives of the 33 crew members aboard the *El Faro*.

There being no objection, the Senate proceeded to consider the resolution.

Mr. MCCONNELL. Mr. President, I ask unanimous consent that the resolution be agreed to, the preamble be agreed to, and the motions to reconsider be laid upon the table with no intervening action or debate.

The PRESIDING OFFICER. Without objection, it is so ordered.

The resolution (S. Res. 291) was agreed to.

The preamble was agreed to.

(The resolution, with its preamble, is printed in today's RECORD under ''Submitted Resolutions.'')

COMMEMORATING THE DISCOVERY OF THE POLIO VACCINE

Mr. MCCONNELL. Mr. President, I ask unanimous consent that the HELP Committee be discharged from further consideration of S. Res. 108 and the Senate proceed to its immediate consideration.

The PRESIDING OFFICER. Without objection, it is so ordered.

The clerk will report the resolution by title.

The bill clerk read as follows:

A resolution (S. Res. 108) commemorating the discovery of the polio vaccine and supporting efforts to eradicate the disease.

There being no objection, the Senate proceeded to consider the resolution.

Mr. MCCONNELL. Mr. President, I ask unanimous consent that the resolution be agreed to, the preamble be agreed to, and the motions to reconsider be considered made and laid upon the table with no intervening action or debate.

The PRESIDING OFFICER. Without objection, it is so ordered.

The resolution (S. Res. 108) was agreed to.

The preamble was agreed to.

(The resolution, with its preamble, is printed in the RECORD of March 24, 2015, under ''Submitted Resolutions.'')

MEASURE READ THE FIRST TIME—S. 2193

Mr. MCCONNELL. Mr. President, I understand there is a bill at the desk, and I ask for its first reading.

The PRESIDING OFFICER. The clerk will read the bill by title for the first time.

The bill clerk read as follows:

A bill (S. 2193) to amend the Immigration and Nationality Act to increase penalties for individuals who illegally reenter the United States after being removed and for other purposes.

Mr. MCCONNELL. I now ask for a second reading and, in order to place the bill on the calendar under the provisions of rule XIV, I object to my own request.

The PRESIDING OFFICER. Objection having been heard, the bill will be read for the second time on the next legislative day.

ORDERS FOR THURSDAY, OCTOBER 22, 2015

Mr. MCCONNELL. Mr. President, I ask unanimous consent that when the Senate completes its business today, it adjourn until 10 a.m., Thursday, October 22; that following the prayer and pledge, the morning hour be deemed expired, the Journal of proceedings be approved to date, and the time for the two leaders be reserved for their use later in the day; that following leader remarks, the Senate resume consideration of S. 754, with the time until 11 a.m. equally divided between the two leaders or their designees; finally, that the filing deadline for all second-degree