113TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPORT
113–324

CRITICAL INFRASTRUCTURE RESEARCH AND DEVELOPMENT ADVANCEMENT ACT OF 2013

JANUARY 9, 2014.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. MCCAUL, from the Committee on Homeland Security, submitted the following

R E P O R T

[To accompany H.R. 2952]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security, to whom was referred the bill (H.R. 2952) to amend the Homeland Security Act of 2002 to make certain improvements in the laws relating to the advancement of security technologies for critical infrastructure protection, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Critical Infrastructure Research and Development Advancement Act of 2013" or the "CIRDA Act of 2013".

SEC. 2. DEFINITIONS.

Section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101) is amended by redesignating paragraphs (15) through (18) as paragraphs (16) through (19), respectively, and by inserting after paragraph (14) the following:

"(15) The term 'Sector Coordinating Council' means a private sector coordinating council that is—

"(A) recognized by the Secretary as such a Council for purposes of this Act; and

"(B) comprised of representatives of owners and operators of critical infrastructure within a particular sector of critical infrastructure.".

SEC. 3. CRITICAL INFRASTRUCTURE PROTECTION RESEARCH AND DEVELOPMENT.

(a) STRATEGIC PLAN; PUBLIC-PRIVATE CONSORTIUMS.—

(1) IN GENERAL.—Title III of the Homeland Security Act of 2002 (6 U.S.C. 181 et seq.) is amended by adding at the end the following:

"SEC. 318. RESEARCH AND DEVELOPMENT STRATEGY FOR CRITICAL INFRASTRUCTURE PROTECTION.

"(a) IN GENERAL.—Not later than 180 days after the date of enactment of the Critical Infrastructure Research and Development Advancement Act of 2013, the Secretary, acting through the Under Secretary for Science and Technology, shall transmit to Congress a strategic plan to guide the overall direction of Federal physical security and cybersecurity technology research and development efforts for protecting critical infrastructure, including against all threats. Once every 2 years after the initial strategic plan is transmitted to Congress under this section, the Secretary shall transmit to Congress an update of the plan.

"(b) CONTENTS OF PLAN.—The strategic plan shall include the following:

"(1) An identification of critical infrastructure security risks and any associated security technology gaps, that are developed following—

"(A) consultation with stakeholders, including the Sector Coordinating Councils; and

"(B) performance by the Department of a risk/gap analysis that considers information received in such consultations.

"(2) A set of critical infrastructure security technology needs that—

"(A) is prioritized based on risk and gaps identified under paragraph (1);

"(B) emphasizes research and development of those technologies that need to be accelerated due to rapidly evolving threats or rapidly advancing infrastructure technology; and

"(C) includes research, development, and acquisition roadmaps with clearly defined objectives, goals, and measures.

"(3) An identification of laboratories, facilities, modeling, and simulation capabilities that will be required to support the research, development, demonstration, testing, evaluation, and acquisition of the security technologies described in paragraph (2).

"(4) An identification of current and planned programmatic initiatives for fostering the rapid advancement and deployment of security technologies for critical infrastructure protection. The initiatives shall consider opportunities for public-private partnerships, intragovernment collaboration, university centers of excellence, and national laboratory technology transfer.

"(5) A description of progress made with respect to each critical infrastructure security risk, associated security technology gap, and critical infrastructure technology need identified in the preceding strategic plan transmitted under this section.

"(c) COORDINATION.—In carrying out this section, the Under Secretary for Science and Technology shall coordinate with the Under Secretary for the National Protection and Programs Directorate.

"(d) CONSULTATION.—In carrying out this section, the Under Secretary for Science and Technology shall consult with—

"(1) the critical infrastructure Sector Coordinating Councils;

"(2) to the extent practicable, subject matter experts on critical infrastructure protection from universities, colleges, including historically black colleges and universities, Hispanic-serving institutions, and tribal colleges and universities, national laboratories, and private industry;

"(3) the heads of other relevant Federal departments and agencies that conduct research and development for critical infrastructure protection; and

"(4) State, local, and tribal governments as appropriate.

"SEC. 319. REPORT ON PUBLIC-PRIVATE RESEARCH AND DEVELOPMENT CONSORTIUMS.

"(a) IN GENERAL.—Not later than 180 days after the enactment of the Critical Infrastructure Research and Development Advancement Act of 2013, the Secretary, acting through the Under Secretary for Science and Technology, shall transmit to Congress a report on the Department's utilization of public-private research and development consortiums for accelerating technology development for critical infrastructure protection. Once every 2 years after the initial report is transmitted to Congress under this section, the Secretary shall transmit to Congress an update of the report. The report shall focus on those aspects of critical infrastructure protection that are predominately operated by the private sector and that would most benefit from rapid security technology advancement.

"(b) CONTENTS OF REPORT.—The report shall include—

"(1) a summary of the progress and accomplishments of on-going consortiums for critical infrastructure security technologies;

"(2) in consultation with the Sector Coordinating Councils and, to the extent practicable, in consultation with subject-matter experts on critical infrastructure protection from universities, colleges, including historically black colleges and universities, Hispanic-serving institutions, and tribal colleges and universities, national laboratories, and private industry, a prioritized list of technology development focus areas that would most benefit from a public-private research and development consortium; and

"(3) based on the prioritized list developed under paragraph (2), a proposal for implementing an expanded research and development consortium program, including an assessment of feasibility and an estimate of cost, schedule, and milestones.".

(2) LIMITATION ON PROGRESS REPORT REQUIREMENT.—Subsection (b)(5) of section 318 of the Homeland Security Act of 2002, as amended by paragraph (1) of this subsection, shall not apply with respect to the first strategic plan transmitted under that section.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by adding at the end of the items relating to such title the following:

"Sec. 318. Research and development strategy for critical infrastructure protection.
"Sec. 319. Report on public-private research and development consortiums.".

(c) CRITICAL INFRASTRUCTURE PROTECTION TECHNOLOGY CLEARINGHOUSE.—Section 313 of the Homeland Security Act of 2002 (6 U.S.C. 193) is amended by redesignating subsection (c) as subsection (d), and by inserting after subsection (b) the following:

"(c) CRITICAL INFRASTRUCTURE PROTECTION TECHNOLOGY CLEARINGHOUSE.—

"(1) DESIGNATION.—Under the program required by this section, the Secretary, acting through the Under Secretary for Science and Technology, and in coordination with the Under Secretary for the National Protection and Programs Directorate, shall designate a technology clearinghouse for rapidly sharing proven technology solutions for protecting critical infrastructure.

"(2) SHARING OF TECHNOLOGY SOLUTIONS.—Technology solutions shared through the clearinghouse shall draw from Government-furnished, commercially furnished, and publically available trusted sources.

"(3) TECHNOLOGY METRICS.—All technologies shared through the clearinghouse shall include a set of performance and readiness metrics to assist end-users in deploying effective and timely solutions relevant for their critical infrastructures.

"(4) REVIEW BY PRIVACY OFFICER.—The Privacy Officer of the Department appointed under section 222 shall annually review the clearinghouse process to evaluate its consistency with fair information practice principles issued by the Privacy Officer.".

(d) EVALUATION OF TECHNOLOGY CLEARINGHOUSE BY GOVERNMENT ACCOUNTABILITY OFFICE.—Not later than 2 years after the date of enactment of this Act, the Comptroller General of the United States shall conduct an independent evaluation of, and submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on, the effectiveness of the clearinghouses established and designated, respectively, under section 313 of the Homeland Security Act of 2002, as amended by this section.

SEC. 4. NO ADDITIONAL AUTHORIZATION OF APPROPRIATIONS.

No additional funds are authorized to be appropriated to carry out this Act and the amendments made by this Act, and this Act and such amendments shall be carried out using amounts otherwise available for such purpose.

PURPOSE AND SUMMARY

The purpose of H.R. 2952 is to amend the Homeland Security Act of 2002 to make certain improvements in the laws relating to the advancement of security technologies for critical infrastructure protection, and for other purposes.

BACKGROUND AND NEED FOR LEGISLATION

The Department of Homeland Security (DHS) is responsible for the prevention of, and defense against threats to United States critical infrastructure. Such threats come in many forms and include threats to people, property, and information. The events of September 11, 2001, demonstrated that terrorist attacks on the homeland can occur in unconventional ways and can result in unanticipated consequences to National security posture and economic vitality. The U.S. is fortunate to have a thriving infrastructure that keeps Americans safe, secure, free, and prosperous. But this infrastructure is technologically complex, interdependent, and potentially vulnerable to physical and cyber attack. New security technologies will need to keep pace with rapidly evolving threats and the rapid advancement of the infrastructure itself. Since U.S. infrastructure is primarily owned and operated by the private sector, improved mechanisms are needed to advance government-sponsored research and development (R&D) of critical infrastructure security-related technologies. It is therefore necessary that DHS develop a comprehensive R&D strategy and a set of improved R&D mechanisms to address a broad spectrum of evolving threats to critical infrastructure. The Committee believes that this strategy requires coordination across the Federal Government and must be developed in collaboration with the private sector. Legislation is required for DHS to develop such a strategy, improve R&D mechanisms, and establish and encourage the necessary coordination and collaboration.

H.R. 2952, the Critical Infrastructure Research and Development Advancement Act of 2013, is bipartisan legislation developed from valuable input from stakeholders and subject matter experts across government and industry. This bill provides three major provisions that will help address R&D gaps in critical infrastructure protection. First, the bill directs the Department of Homeland Security to facilitate the development of an R&D strategy for critical infrastructure security technologies. This strategy will help the Federal Government and stakeholders prioritize their investments in those aspects of the infrastructure that are most at risk. Second, the bill requires that DHS study and report on the feasibility of expanding the use of public-private R&D consortiums to accelerate new security technologies and potentially spur innovation and economic competitiveness. Lastly, the bill designates a "technology clearinghouse" where proven security tools for protecting infrastructure can be rapidly shared amongst government and private partners.

HEARINGS

No hearings were held on H.R. 2952. However, the Committee held oversight hearings on programs and threats relevant to H.R. 2952, these hearings are listed below.

112th Congress.

The Subcommittee on Emergency Preparedness, Response, and Communications held a hearing on April 15, 2011, entitled "The DHS Cybersecurity Mission: Promoting Innovation and Securing Critical Infrastructure." The Subcommittee received testimony from Mr. Sean McGurk, Director, National Cybersecurity and Communications Integration Center, Department of Homeland Security; Mr. Gerry Cauley, President and CEO, North American Electric Reliability Corporation; Ms. Jane Carlin, Chair, Financial Services Sector Coordinating Council; and Mr. Edward Amoroso, Senior Vice President and Chief Security Officer, AT&T.

On July 15, 2011, the Subcommittee on Oversight, Investigations, and Management held a hearing entitled "Homeland Security Contracting: Does the Department Effectively Leverage Emerging Technologies?" The Subcommittee received testimony from Mr. Charles K. Edwards, Acting Inspector General, Department of Homeland Security; Mr. David Maurer, Director, Homeland Security and Justice Team, Government Accountability Office; Mr. Rafael Borras, Under Secretary for Management and Chief Acquisition Officer, Department of Homeland Security; Dr. Tara O'Toole, Under Secretary, Science and Technology Directorate, Department of Homeland Security; Mr. Jim Williams, Vice Chair, Homeland Security Committee, TechAmerica; Mr. Marc Pearl, President and CEO, Homeland Security and Defense Business Council; and Mr. Scott Amey, General Counsel, Project On Government Oversight.

On November 17, 2011 the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies held a hearing entitled "S&T on a Budget: Finding Smarter Approaches to Spur Innovation, Impose Discipline, Drive Job Creation, and Strengthen Homeland Security." The Subcommittee received testimony from Hon. Tara O'Toole, Under Secretary, Science and Technology Directorate, Department of Homeland Security; and Mr. David C. Maurer, Director, Homeland Security and Justice Issues, Government Accountability Office.

On February 3, 2012, the Subcommittee on Oversight, Investigations, and Management held a hearing entitled "Is DHS Effectively Implementing a Strategy to Counter Emerging Threats?" The Subcommittee received testimony from Hon. Paul Schneider, Principal, The Chertoff Group; Ms. Sharon L. Caudle, PhD, The Bush School of Government and Public Service, Texas A&M University; Mr. Shawn Reese, Analyst, Emergency Management and Homeland Security Policy, Congressional Research Service; Mr. David Maurer, Director, Homeland Security and Justice Team, Government Accountability Office; and Mr. Alan Cohn, Deputy Assistant Secretary, Office of Policy, Department of Homeland Security.

On April 19, 2012, the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies held a hearing entitled "The DHS and DOE National Labs: Finding Efficiencies and Optimizing Outputs in Homeland Security Research and Development." The Subcommittee received testimony from Dr. Daniel M.

Gerstein, Deputy Under Secretary for Science and Technology, Department of Homeland Security; Dr. Huban Gowadia, Deputy Director, Domestic Nuclear Detection Office, Department of Homeland Security; Dr. Daniel Morgan, Specialist in Science and Technology Policy, Resources, Sciences, and Industry Division, Congressional Research Service; Ms. Jill Hruby, Vice President, International, Homeland and Nuclear Security, Sandia National Laboratories; and Dr. Michael Robert Carter, Senior Scientist, National Ignition Facility and Photon Science Directorate, Lawrence Livermore National Laboratory.

On April 26, 2012, the Subcommittee on Counterterrorism and Intelligence and the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies held a joint hearing entitled "Iranian Cyber Threat to the U.S. Homeland." The Subcommittees received testimony from Mr. Frank J. Cilluffo, Associate Vice President and Director, Homeland Security Policy Institute, The George Washington University; Mr. Ilan Berman, Vice President, American Foreign Policy Council; and Mr. Roger Caslow, Executive Cyberconsultant, Suss Consulting.

On September 20, 2012, the Full Committee held a hearing entitled "The Department of Homeland Security: An Assessment of the Department and a Roadmap for its Future." The Committee received testimony from Hon. Richard L. Skinner, Former Inspector General, Department of Homeland Security; Hon. Stewart A. Baker, Former Assistant Secretary for Policy, Department of Homeland Security; Mr. Frank J. Cilluffo, Former Principal Advisor to Governor Tom Ridge, White House Office of Homeland Security; Mr. David C. Maurer, Director, Homeland Security and Justice, Government Accountability Office.

113th Congress.

On March 13, 2013, the Full Committee held a hearing entitled "DHS Cybersecurity: Roles and Responsibilities to Protect the Nation's Critical Infrastructure." The Committee received testimony from Hon. Jane Holl Lute, Deputy Secretary, U.S. Department of Homeland Security; Mr. Anish B. Bhimani, Chairman, Financial Services Information Sharing and Analysis Center; Mr. Gary W. Hayes, Chief Information Officer, Centerpoint Energy; and Ms. Michelle Richardson, Legislative Counsel, American Civil Liberties Union.

On March 20, 2013, the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies held a hearing entitled "Cyber Threats from China, Russia and Iran: Protecting American Critical Infrastructure." The Subcommittee received testimony from Mr. Frank J. Cilluffo, Director, Homeland Security Policy Institute and Co-Director, Cyber Center for National and Economic Security, The George Washington University; Mr. Richard Bejtlich, Chief Security Officer and Security Services Architect, Mandiant; Mr. Ilan Berman, Vice President, American Foreign Policy Council; and Mr. Martin C. Libicki, Senior Management Scientist, RAND Corporation.

On April 25, 2013, the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies held a hearing entitled "Striking the Right Balance: Protecting Our Nation's Critical Infrastructure from Cyber Attack and Ensuring Privacy and Civil Liberties." The Subcommittee received testimony from Ms. Mary

Ellen Callahan, Partner, Jenner & Block and Former Chief Privacy Officer, U.S. Department of Homeland Security; Ms. Cheri F. McGuire, Vice President, Global Government Affairs & Cybersecurity Policy, Symantec; and Ms. Harriet Pearson, Partner, Hogan Lovells.

On May 16, 2013, the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies held a hearing entitled "Facilitating Cyber Threat Information Sharing and Partnering with the Private Sector to Protect Critical Infrastructure: An Assessment of DHS Capabilities." The Subcommittee received testimony from Ms. Roberta Stempfley, Acting Assistant Secretary, Office of Cybersecurity and Communications, U.S. Department of Homeland Security; Mr. Larry Zelvin, Director, National Cybersecurity and Communications Integration Center, U.S. Department of Homeland Security; and Mr. Charles K. Edwards, Acting Inspector General, U.S. Department of Homeland Security.

On July 18, 2013, the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies held a hearing entitled "Oversight of Executive Order 13636 and Development of the Cybersecurity Framework." The Subcommittee received testimony from Mr. Robert Kolasky, Director, Implementation Task Force, National Protection and Programs Directorate, U.S. Department of Homeland Security; Charles H. Romine, PhD, Director, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce; and Eric A. Fischer, PhD, Senior Specialist, Science and Technology, Congressional Research Service, Library of Congress.

COMMITTEE CONSIDERATION

The Committee on Homeland Security met on October 29, 2013, to consider H.R. 2952, and ordered the measure to be reported to the House with a favorable recommendation by voice vote. The Committee took the following actions:

The Committee agreed to H.R. 2952, as amended, by voice vote.

The following amendments were offered:

An Amendment in the Nature of a Substitute to H.R. 2952 offered by MRS. BROOKS *on behalf of* MR. MEEHAN (#1); was AGREED TO, as amended, by voice vote.

A unanimous consent request by Mr. McCaul to consider the Amendment in the Nature of a Substitute as base text for purposes of amendment was not objected to.

An amendment to the Amendment in the Nature of a Substitute to H.R. 2952 offered by Ms. Jackson Lee (#1A); was AGREED TO by voice vote.

> Page 2, line 17, after " protecting critical infrastructure" insert ", including against all threats".

An amendment to the Amendment in the Nature of a Substitute to H.R. 2952 offered by Ms. Jackson Lee (#1B); was WITHDRAWN by unanimous consent.

> Add at the end a new section entitled "Sec. __. Assessment and Report on Vulnerabilities and Threats on Computer Systems."

The Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies met on September 18, 2013, to consider H.R. 2952, and ordered the measure reported to the Full Com-

mittee with a favorable recommendation, as amended, by voice vote. The Subcommittee took the following actions:

The following amendments were offered:

An amendment by MR. MEEHAN (#1); was AGREED TO by voice vote.

Page 3, line 9, strike "the" and insert "any".

Page 5, beginning at line 16, strike "study on the use by the Department" and insert "report on the Department's utilization".

Page 5, line 20, strike "study" and insert "report".

Page 5 line 22, strike "study. The study" and insert "report. The Report".

Page 6, line 1, strike "Study.—The study" and insert "Report.—The report".

Page 7, beginning at line 18, strike "metrics to assist end-users in deploying timely and effective" and insert "performance and readiness metrics to assist end-users in deploying effective and timely"

An amendment by MS. CLARKE (#2); was AGREED TO by voice vote.

Page 2, line 16, strike "(a) In General.—" and insert the following: "(a) Strategic Plan; Public-private Consortiums.—

(1) In general.—

Page 4, after line 16, insert a new paragraph (5).

Page 6, after line 15, insert a new section "(2) Limitation on progress report requirement.—"

An amendment by MR. KEATING (#1); was WITHDRAWN by unanimous consent.

Page 6, strike the closing quotation marks and the second period at line 15, and after line 15 insert a new section entitled "Sec. 320. Identification of Cybersecurity Risks to the Nuclear Reactors, Materials, and Waste Sector."

Page 6, in the matter following line 18, in the item relating to section 319 strike the closing quotation marks and the section period, and after such item insert the following: "Sec. 320. Identification of Cybersecurity Risks to the Nuclear Reactors, Materials, and Waste Sector."

COMMITTEE VOTES

Clause 3(b) of rule XIII of the Rules of the House of Representatives requires the Committee to list the recorded votes on the motion to report legislation and amendments thereto.

No recorded votes were requested during consideration of H.R. 2952.

COMMITTEE OVERSIGHT FINDINGS

Pursuant to clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee has held oversight hearings and made findings that are reflected in this report.

NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

In compliance with clause 3(c)(2) of rule XIII of the Rules of the House of Representatives, the Committee finds that H.R. 2952, the Critical Infrastructure Research and Development Advancement Act of 2013, would result in no new or increased budget authority, entitlement authority, or tax expenditures or revenues.

CONGRESSIONAL BUDGET OFFICE ESTIMATE

The Committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, November 6, 2013.

Hon. MICHAEL MCCAUL,
Chairman, Committee on Homeland Security,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 2952, the Critical Infrastructure Research and Development Advancement Act of 2013.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Mark Grabowicz.

Sincerely,

DOUGLAS W. ELMENDORF.

Enclosure.

H.R. 2952—Critical Infrastructure Research and Development Advancement Act of 2013

CBO estimates that implementing H.R. 2952 would have discretionary costs totaling less than $500,000 in each of fiscal years 2014 and 2015. Enacting the legislation would not affect direct spending or revenues; therefore, pay-as-you-go procedures do not apply.

The bill would require the Department of Homeland Security (DHS), within 180 days of the bill's enactment, to transmit to the Congress a strategic plan for research and development efforts addressing the protection of critical infrastructure and a report on departmental use of public-private consortiums to develop technology to protect such infrastructure. The bill also would direct the Government Accountability Office (GAO), within two years of enactment, to evaluate the effectiveness of clearinghouses established by DHS to share technological innovation. Based on the cost of similar activities, CBO estimates the DHS and GAO reports required by H.R. 2952 would cost less than $500,000 annually in 2014 and 2015, assuming availability of appropriated funds.

H.R. 2952 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act and would not affect the budgets of state, local, or tribal governments.

The CBO staff contact for this estimate is Mark Grabowicz. The estimate was approved by Theresa Gullo, Deputy Assistant Director for Budget Analysis.

STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, H.R. 2952 contains the following general performance goals, and objectives, including outcome related goals and objectives authorized.

The performance goals and objectives of H.R. 2952 are based on the development of a critical infrastructure research and development (R&D) plan and the identification of improvements to DHS R&D mechanisms. The goal of the R&D strategic plan required under H.R. 2952 is to help guide the overall direction of Federal physical security and cybersecurity technology R&D for protecting critical infrastructure. The performance objective of the R&D plan is to establish and communicate critical infrastructure security

risks, gaps, and associated technology solutions, and measure progress towards that end. The goal of the report on public-private R&D consortiums required under H.R. 2952 is to aid in the acceleration of critical infrastructure security technologies through public-private collaboration. The objective of this consortium report is to measure progress on current consortiums and to establish the merits of expanding the consortium mechanism to improve DHS's R&D performance. Finally, the goal of designating a technology clearinghouse for critical infrastructure protection is to establish a focused mechanism for sharing information on proven security technologies between public and private entities. The performance objective of this clearinghouse is to assist end-users in deploying effective and timely solutions for their relevant critical infrastructures. The Congressional reports from DHS and the Government Accountability Office (GAO) that are required by this Act will allow the Congress to hold the Department accountable for the success or failure of its critical infrastructure protection R&D programs.

DUPLICATIVE FEDERAL PROGRAMS

The Committee finds that H.R. 2952 does not contain any provision that establishes or reauthorizes a program known to be duplicative of another Federal program.

CONGRESSIONAL EARMARKS, LIMITED TAX BENEFITS, AND LIMITED TARIFF BENEFITS

In compliance with rule XXI of the Rules of the House of Representatives, this bill, as reported, contains no congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9(e), 9(f), or 9(g) of the rule XXI.

FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

PREEMPTION CLARIFICATION

In compliance with section 423 of the Congressional Budget Act of 1974, requiring the report of any Committee on a bill or joint resolution to include a statement on the extent to which the bill or joint resolution is intended to preempt State, local, or Tribal law, the Committee finds that H.R. 2952 does not preempt any State, local, or Tribal law.

DISCLOSURE OF DIRECTED RULE MAKINGS

The Committee estimates that H.R. 2952 would require no directed rule makings.

ADVISORY COMMITTEE STATEMENT

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act were created by this legislation.

APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short Title.

This section provides that the bill may be cited as the "Critical Infrastructure Research and Development Advancement Act of 2013" or "the CIRDA Act of 2013."

Section 2. Definitions.

In this section, Section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101) is amended to include a definition for "Sector Coordinating Council." The term "Sector Coordinating Council", or "SCC", is defined as a private sector coordinating council, comprised of representatives of owners and operators of critical infrastructure within a particular sector of critical infrastructure, which is recognized by the Secretary for purposes of this Act. The Sector Coordinating Councils are an existing construct established under presidential directives to develop and implement a National Infrastructure Protection Plan (NIPP). As of the writing of this report, there are 16 critical infrastructure sectors and 16 corresponding SCC's defined under the NIPP. The purpose of defining Sector Coordinating Councils in this bill is to codify into statute the role of such councils in informing the Federal government on critical infrastructure protection issues relevant to the research and development (R&D) of security-related technologies.

The Committee believes that the Federal government needs to closely partner with the private sector during the establishment and implementation of a risk-informed R&D strategy. The Committee also believes that the SCC's should serve as the private-sector body that enables small, medium, and large businesses within each sector to inform the R&D strategy and to communicate progress on emerging critical infrastructure protection technologies.

Since this bill only addresses the R&D aspects of critical infrastructure protection, it is the Committee's intent that the basic definition described in this section will suffice for such purposes. However, the Committee recognizes that SCC's have a significantly broader role in critical infrastructure protection and that the definition herein may not suffice for those broader purposes. Therefore, the Committee strongly encourages the Secretary to develop a set of effective and efficient Departmental processes for defining, designating, and interfacing with Sector Coordinating Councils to support the broad critical infrastructure protection mission.

Section 3. Critical Infrastructure Protection Research and Development.

This section amends Title III of the Homeland Security Act of 2002 (6 U.S.C. 181 et seq.) by adding a new Section 318 and a new Section 319.

Sec. 318. Research and Development Strategy for Critical Infrastructure Protection.

(a) In General.

This subsection requires the Secretary, acting through the Undersecretary for Science and Technology (S&T), to develop and submit to Congress a strategic plan for guiding the direction of Federal physical security and cyber technology R&D efforts to protect critical infrastructure against all threats. The plan is due to Congress 180 days after enactment and every 2 years thereafter.

Based on extensive oversight, the Committee has found that there currently is no comprehensive National strategy for the R&D of security technologies for protecting critical infrastructure. While recent efforts by the Executive branch have attempted to include R&D in the National Infrastructure Protection Plan, the Committee believes that roles, responsibilities, and accountabilities are currently ill-defined. It is the intent of the Committee that DHS, because of its statutory authorities for critical infrastructure protection, needs to provide the necessary leadership and facilitation of such a National R&D strategy. Similarly, the Committee believes that DHS S&T, because of its statutory authorities established under Title III, needs to be the primary facilitator within the Department for such a National R&D strategy.

(b) Contents of Plan.

In this subsection, the contents of the R&D strategic plan are prescribed. The contents prescribed are the minimum contents required, however, the Committee strongly encourages DHS to include other aspects necessary for effective multi-year planning. The Committee expects that each of the prescribed elements in the plan be developed and published in sufficient detail to enable DHS and the public/private stakeholders to adequately plan for future technology investments. While the timeline of the plan is not specified in the bill, the Committee strongly encourages DHS to address near-term (e.g. 1–3 years), mid-term (e.g. 3–7 years), and long-term (e.g. 8 years and beyond) aspects in the plan. The Committee furthermore expects DHS to write the plan in an organized hierarchal manner structured around risk-based objectives, goals, and measures.

The plan is to include an identification of critical infrastructure risks and an identification of any associated security technology gaps. DHS is to identify these risks and gaps by first consulting with stakeholders, including the Sector Coordinating Councils. Since the critical infrastructure is largely owned and operated by the private sector, the Committee believes that it is absolutely necessary for DHS to proactively engage with these owners/operators, through the SCC's and other mechanisms, in order to effectively identify risks and gaps. The Committee also believes that the risk identification needs to consider all threats to critical infrastructure, whether they be from terrorist attack or natural disaster. Furthermore, the Committee believes that the risk identification needs to consider both physical and cyber aspects, including potential vulnerabilities to control systems, computer systems, firewalls, and software.

The plan is to include a set of critical infrastructure technology needs that are prioritized based on the risks and gaps identified in the plan. The Committee expects DHS to develop this plan in a manner that is not constrained by fiscal resources, and therefore needs to identify all potential technology solutions. Once these set of solutions are identified, however, the Committee notes that it is important for DHS to prioritize these so that they can be included in the OMB multi-year budget planning process. When identifying the set of prioritized technology needs, the bill requires DHS to emphasize the R&D of those technologies that need to be accelerated due to rapidly evolving threats or rapidly advancing infrastructure itself. Since the bill covers both physical security and cybersecurity aspects for critical infrastructure, the Committee strongly encourages DHS to consider the appropriate balance between physical and cybersecurity priorities. At the time of writing this report, the Committee believes that cyber threats are rapidly evolving and cyber infrastructure is rapidly advancing, thereby necessitating a greater emphasis in such a plan at this time. When identifying the set of prioritized technologies, the bill also requires DHS to include research, development, and acquisition roadmaps with clearly defined objectives, goals and measures. The Committee strongly encourages DHS to establish roadmaps in a manner that is consistent with industry and government best practices for technology management. Specifically, the Committee expects that the roadmaps will provide sufficient detail to enable potential technology developers to plan for the basic research, engineering development, and acquisition phases of the prioritized security technologies. The Committee also strongly encourages DHS to utilize standardized terminology and metrics when publishing these roadmaps. Specifically, the Committee strongly encourages DHS to adopt the 9-level technology readiness level (TRL) scale that has been recognized as a best practice by the GAO, NASA, DoD, and DOE.

The plan is to include an identification of laboratories, facilities, modeling, and simulation capabilities required to support the maturation of the security technologies identified in the plan. The Committee believes that it is very important that DHS identify the laboratories, facilities and capabilities in order to ensure that these assets are available when needed. The Committee also believes that it is necessary for DHS to identify potential gaps in these assets to aid in the planning of new facility construction, laboratory retrofitting, or design and development of new modeling/simulation capabilities. The Committee encourages DHS to consider government assets in the plan and also include third-party assets that could be leveraged from private industry, National Laboratories, or academia. The Committee strongly recommends that DHS S&T include laboratories, facilities, modeling, and simulation aspects in all of its strategic plans that it develops in support of the DHS mission.

The plan is to include an identification of current and planned initiatives for fostering the rapid advancement and deployment of security technologies for critical infrastructure protection. These initiatives include opportunities for public-private partnerships, intra-government collaboration, university centers of excellence, and National Laboratory technology transfer. The Committee believes that new technology R&D models are needed for critical in-

frastructure due to the highly interdisciplinary and interdependent nature of the problem. For example, under the category of public-partnerships, the Committee believes that R&D consortiums are a potential candidate for accelerating innovation, and is a topic that is expanded upon in Section 319. As another example, the Committee believes that a potential candidate for intra-government collaboration would involve an R&D partnership between DHS and the Department of Energy, through their National Laboratories, to accelerate the R&D of energy-related critical infrastructure security technologies. The Committee strongly encourages DHS S&T to seriously consider alternative R&D models for critical infrastructure protection and to implement new programs to support these initiatives.

The plan is to include a description of progress made towards the elements described in the preceding version of the strategic plan. The Committee believes that it is critically important that DHS implement the strategic plan that it develops. The Committee also recognizes that plans can change due to unforeseen circumstances, and encourages DHS to actively update and republish the plan regularly as needed.

The Committee recognizes that DHS S&T, as of the writing of this report, is actively engaging with several DHS components to develop strategic R&D plans. The Committee fully supports the Department's coordination efforts and strongly encourages the continuation of these strategic planning activities. It is the Committee's intent that the Congressional report required under this section leverages, and not duplicate, the strategic R&D planning activities already being implemented at DHS.

(c) Coordination.

This subsection requires DHS S&T to coordinate with the National Protection and Programs Directorate (NPPD) in implementing this section of the bill. Since NPPD serves as the Department's operational component for critical infrastructure protection, the Committee believes that it is absolutely necessary that S&T and NPPD coordinate to the greatest extent possible to plan and implement the R&D strategy. Based on extensive oversight conducted by the Committee, the Committee believes that S&T and NPPD have not been effectively coordinating their R&D-related activities and need to significantly improve in this regard. The Committee notes that this lack of coordination is particularly acute in the research, development, testing, evaluation, and acquisition of cyber-security technologies. The intent of the Committee is to require such coordination under statute in order to ensure that such coordination occurs.

(d) Consultation.

This subsection requires that DHS S&T consult with multiple entities in implementing this section of the bill. The Committee strongly encourages that DHS consult and collaborate with the owners and operators of critical infrastructure, as represented through the Sector Coordinating Councils. Furthermore, the Committee strongly encourages that DHS consult with a broad cross-section of subject matter experts on critical infrastructure protection from the private sector, National Laboratories, and academia.

The Committee recognizes that such broad subject matter expert engagement has certain logistical challenges, but encourages DHS to use innovative means such as workshops, social media, and webinars to carry out such consultation. The bill also requires consultation with other Federal Departments and agencies that conduct R&D for critical infrastructure. The Committee expects DHS S&T to provide the Federal leadership role in facilitating a National R&D strategy, and the Committee believes that such intragovernment consultation is absolutely necessary. The Committee notes that other branches of the Federal government that conduct critical infrastructure protection R&D include: DOE, DoD, NIST, and NSF. Finally, this subsection requires appropriate consultation with State, local, and Tribal governments. The Committee believes that State, local, and Tribal entities have an important role in preparedness and emergency response to critical infrastructure incidents and that their perspectives and needs are an important consideration in the development of the R&D strategy. The Committee notes that State and local entities include port authroities.

Sec. 319. Report on Public-Private Research and Development Consortiums.

(a) In General.

This subsection requires the Secretary, acting through the Undersecretary for S&T, to develop and transmit to Congress a report on the Department's utilization of public-private research and development consortiums for accelerating technology development for critical infrastructure protection. The report is due 180 days after enactment of the bill and updated every 2 years thereafter. The bill requires that the report focus on those aspects of critical protection that are predominately operated by the private sector and would benefit from rapid security technology development.

The Committee believes that DHS has underutilized public-private R&D partnerships in its overall science and technology strategy. The Technology Transfer Commercialization Act of 2000 (Pub. L. 106–404) and other related legislation, provides the Federal government the necessary mechanisms to conduct public-private shared R&D. While DHS has implemented some public-private R&D consortiums, they have tended to be small (several million dollars or less), and managed through non-private third-party entities. The Committee believes that DHS needs to expand its consideration of public-private R&D consortiums, especially in areas that are mutually beneficial between the two sectors. The Committee notes that critical infrastructure protection, because of significant private-sector stakeholder interest, would greatly benefit from increased use of improved R&D consortiums. When implementing Section 319, the Committee strongly encourages DHS to develop an implementation plan for expanding the use of public-private R&D consortiums for critical infrastructure protection.

(b) Contents of Report.

In this subsection, the contents of the public-private R&D consortium report are prescribed. The contents prescribed therein are the minimum contents and it is the Committee's expectation that DHS will include additional content as necessary to enable effective con-

sortium planning. It is the Committee's intent that this report is to complement the R&D strategy report prescribed under Section 318. The Committee strongly encourages DHS to develop and transmit these two reports in tandem and avoid any unnecessary duplication within the two reports.

The consortium report is to include a summary of the progress and accomplishments of on-going R&D consortiums for critical infrastructure security technologies. The Committee encourages DHS to establish objectives, goals, and measures for each of its R&D consortium projects in the context of the strategic plan prescribed under Section 318.

The consortium report is to include, in consultation with stakeholders and subject matter experts, a prioritized list of technology development focus areas that would benefit from a public-private R&D consortium. In developing this prioritized list, the Committee strongly encourages DHS to utilize the risk-based analyses and the stakeholder consultations conducted under Section 318. The Committee also encourages DHS to look holistically at R&D consortium focus opportunities and consider both physical security technologies and cybersecurity technologies. As of the writing of this report, the Committee believes that cybersecurity R&D may be particularly appropriate for expanded R&D partnership opportunities. Specifically, the Committee believes that a cybersecurity protection and prevention R&D consortium would generate substantial interest from both the public and the private sectors.

The consortium report is to include a prioritized proposal for implementing an expanded R&D consortium program. This proposal is to include an assessment of feasibility and an estimate of cost, schedule and milestones. It is the Committee's intent that DHS establish such a proposal and then seek Congressional authorization and appropriation to implement such a proposed expanded program. Although the bill does not prescribe how such a consortium should be constructed, the Committee strongly encourages DHS to include a working partnership model in its R&D consortium proposal. The Committee believes that the consortium model should include the following key attributes: (1) The model draws upon industry, academic, and government best-practices for successful R&D consortiums; (2) the model encourages active participation and leadership by the private sector, while streamlining government administrative overhead; (3) the model provides matching funding for R&D projects, with the U.S. Government's funding contributions not exceeding 50 percent; (4) the model leverages security technology investments made by other departments and agencies of the Federal government; (5) the model leverages and encourages technology transfer from National Laboratories and academia; and (6) the model provides a mechanism for accelerating technology certification under subtitle G of title VII (known as the "SAFETY Act").

(c) Critical Infrastructure Protection Technology Clearinghouse.

(1) Designation.

This subsection amends Section 313 of the Homeland Security Act 2002 and requires requires the Secretary, acting through the Undersecretary for S&T, and in coordination with the Undersecre-

tary for NPPD, to designate a focused technology clearinghouse within the clearinghouse program required under Section 313. The designated technology clearinghouse is to focus on the rapid sharing of proven technology solutions for protecting critical infrastructure. The Congressional intent of this subsection is twofold: Firstly, to authorize the DHS, through a designated clearinghouse, to focus on the Department's mission in critical infrastructure protection; and secondly, to ensure that the designated technology clearinghouse is well coordinated between the Science and Technology Directorate and the operational mission of the National Protection and Program Directorate.

The Committee believes that DHS has underutilized the clearinghouse mechanism established under Section 313. Specifically, Section 313 requires "The establishment of a centralized Federal clearinghouse for information relating to technologies that would further the mission of the Department for dissemination, as appropriate, to Federal, State, and local government and private sector entities for additional review, purchase, or use." Based on Committee oversight, the Committee has found that DHS has not established such a Federal-wide clearinghouse, and that the current clearinghouse is only used to gather first responder requirements. The clearinghouse does not currently disseminate information on mission-relevant technologies, and does not provide a technology information sharing mechanism for the private sector, as statutorily required. The Committee further believes that DHS has under-resourced the clearinghouse program and that its information sharing mechanism, which is a simple website, has been largely ineffective. Therefore, the Committee strongly encourages DHS to increase and improve its utilization of the clearinghouse mechanism to meet the statutory requirements. The Committee believes that focused clearinghouses, such as the critical infrastructure clearinghouse designated in this section, will serve as a driver for DHS to improve its technology information sharing and better coordinate amongst private and public stakeholders.

(2) Sharing of Technology Solutions.

This subsection requires that technology solutions shared through the clearinghouse be drawn from government-furnished, commercially-furnished, and publicly available trusted sources. The Committee believes that DHS does not effectively use the clearinghouse as a technology information sharing mechanism, and this subsection clarifies the Congressional intent that DHS share such information from various sources. When sharing technology solutions through the clearinghouse, the Committee notes that it will be important for DHS to exercise due diligence to ensure that the sources of that information are trustworthy and reputable from a National security perspective.

(3) Technology Metrics.

This subsection requires that all technologies shared (or information about technologies thereof), include a set of performance and readiness metrics. These metrics are required to assist end-users in deploying effective and timely solutions relevant for their critical infrastructures. The Committee believes that metrics are an important aspect in technology information sharing and help security

professionals make objective decisions about which technologies best meet their mission needs. The bill does not specify which specific metrics are required, and allows DHS flexibility in establishing an effective metrics set. However, the Committee believes that these metrics need to be based on industry and government technology management best practices. The Committee also believes that test and evaluation activities should be tied to these metrics. The Committee strongly encourages DHS to improve its implementation of the clearinghouse mechanism, share relevant technology information to the broad stakeholder community, and do so in an objective manner through standardized metrics.

(4) Review by Privacy Officer.

This subsection requires the Privacy Officer of the Department to annually review the clearinghouse process to evaluate its consistency with Fair Information Practice Principles and the Privacy Act of 1974. The Committee believes that security-related technologies need to be developed and deployed in a manner that fully considers privacy and civil liberty implications, including protection of personally identifiable information. The Committee notes that consideration of privacy and civil liberty implications is critically important for cybersecurity and information-based technologies. While the bill does not require that each technology within the clearinghouse be assessed, the Committee expects DHS to establish a process for conducting privacy impact assessments when appropriate.

(d) Evaluation of Technology Clearinghouse by Government Accountability Office.

This subsection requires the GAO to evaluate and report on the effectiveness of the clearinghouses established and designated under Section 313 as amended. The GAO report is to be transmitted to the relevant Congressional committees within 2 years after enactment of the bill. The Committee's intent of this subsection is to direct GAO to gather data, assess DHS's implementation of Section 313, and evaluate the effectiveness and efficiency of the implemented clearinghouses. As stated in a prior section of this report, the Committee believes that DHS does not currently implement technology clearinghouses in a manner consistent with statute, and this independent assessment will inform the Committee on this issue. It is the Committee's belief that the GAO report will provide important inputs for continuing Congressional oversight and provide additional transparency for the American public.

Sec. 4. No Additional Authorization of Appropriations.

This section requires the provisions of this bill to be carried out using amounts otherwise available. The Committee believes that the strategic planning and R&D consortium planning required under this bill represents work that is largely already conducted at DHS. As such, the Committee believes that DHS should appropriately absorb the minimal costs required to improve its R&D strategies, report to Congress, and increase its transparency. The Committee believes that DHS has underutilized technology clearinghouses and has not implemented them in a manner consistent with Congressional intent of the Homeland Security Act of 2002. It

is the Committee's belief that DHS will need to strengthen the clearinghouses in order to comply with existing law, and that costs incurred to do so should be absorbed from lower priority DHS programs. The Committee strongly encourages DHS to implement these provisions in a manner that leads to more effective and efficient R&D programs, thereby resulting in long-term Federal Government savings.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, existing law in which no change is proposed is shown in roman):

HOMELAND SECURITY ACT OF 2002

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Homeland Security Act of 2002".

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

* * * * * * *

TITLE III—SCIENCE AND TECHNOLOGY IN SUPPORT OF HOMELAND SECURITY

* * * * * * *

Sec. 318. Research and development strategy for critical infrastructure protection.
Sec. 319. Report on public-private research and development consortiums.

* * * * * * *

SEC. 2. DEFINITIONS.

In this Act, the following definitions apply:

(1) Each of the terms "American homeland" and "homeland" means the United States.

(2) The term "appropriate congressional committee" means any committee of the House of Representatives or the Senate having legislative or oversight jurisdiction under the Rules of the House of Representatives or the Senate, respectively, over the matter concerned.

(3) The term "assets" includes contracts, facilities, property, records, unobligated or unexpended balances of appropriations, and other funds or resources (other than personnel).

(4) The term "critical infrastructure" has the meaning given that term in section 1016(e) of Public Law 107–56 (42 U.S.C. 5195c(e)).

(5) The term "Department" means the Department of Homeland Security.

(6) The term "emergency response providers" includes Federal, State, and local governmental and nongovernmental emergency public safety, fire, law enforcement, emergency response, emergency medical (including hospital emergency facilities), and related personnel, agencies, and authorities.

(7) The term "executive agency" means an executive agency and a military department, as defined, respectively, in sections 105 and 102 of title 5, United States Code.

(8) The term "functions" includes authorities, powers, rights, privileges, immunities, programs, projects, activities, duties, and responsibilities.

(9) The term "intelligence component of the Department" means any element or entity of the Department that collects, gathers, processes, analyzes, produces, or disseminates intelligence information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, or national intelligence, as defined under section 3(5) of the National Security Act of 1947 (50 U.S.C. 401a(5)), except—

(A) the United States Secret Service; and

(B) the Coast Guard, when operating under the direct authority of the Secretary of Defense or Secretary of the Navy pursuant to section 3 of title 14, United States Code, except that nothing in this paragraph shall affect or diminish the authority and responsibilities of the Commandant of the Coast Guard to command or control the Coast Guard as an armed force or the authority of the Director of National Intelligence with respect to the Coast Guard as an element of the intelligence community (as defined under section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)).

(10) The term "key resources" means publicly or privately controlled resources essential to the minimal operations of the economy and government.

(11) The term "local government" means—

(A) a county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or interstate government entity, or agency or instrumentality of a local government;

(B) an Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and

(C) a rural community, unincorporated town or village, or other public entity.

(12) The term "major disaster" has the meaning given in section 102(2) of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122).

(13) The term "personnel" means officers and employees.

(14) The term "Secretary" means the Secretary of Homeland Security.

(15) The term "Sector Coordinating Council" means a private sector coordinating council that is—

(A) recognized by the Secretary as such a Council for purposes of this Act; and

(B) comprised of representatives of owners and operators of critical infrastructure within a particular sector of critical infrastructure.

[(15)] *(16)* The term "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States.

[(16)] *(17)* The term "terrorism" means any activity that—

(A) involves an act that—

(i) is dangerous to human life or potentially destructive of critical infrastructure or key resources; and

(ii) is a violation of the criminal laws of the United States or of any State or other subdivision of the United States; and

(B) appears to be intended—

(i) to intimidate or coerce a civilian population;

(ii) to influence the policy of a government by intimidation or coercion; or

(iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping.

[(17)] *(18)*(A) The term "United States", when used in a geographic sense, means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, any possession of the United States, and any waters within the jurisdiction of the United States.

(B) Nothing in this paragraph or any other provision of this Act shall be construed to modify the definition of "United States" for the purposes of the Immigration and Nationality Act or any other immigration or nationality law.

[(18)] *(19)* The term "voluntary preparedness standards" means a common set of criteria for preparedness, disaster management, emergency management, and business continuity programs, such as the American National Standards Institute's National Fire Protection Association Standard on Disaster/Emergency Management and Business Continuity Programs (ANSI/NFPA 1600).

* * * * * * *

TITLE III—SCIENCE AND TECHNOLOGY IN SUPPORT OF HOMELAND SECURITY

* * * * * * *

SEC. 313. TECHNOLOGY CLEARINGHOUSE TO ENCOURAGE AND SUPPORT INNOVATIVE SOLUTIONS TO ENHANCE HOMELAND SECURITY.

(a) ESTABLISHMENT OF PROGRAM.—The Secretary, acting through the Under Secretary for Science and Technology, shall establish and promote a program to encourage technological innovation in facilitating the mission of the Department (as described in section 101).

(b) ELEMENTS OF PROGRAM.—The program described in subsection (a) shall include the following components:

(1) The establishment of a centralized Federal clearinghouse for information relating to technologies that would further the

mission of the Department for dissemination, as appropriate, to Federal, State, and local government and private sector entities for additional review, purchase, or use.

(2) The issuance of announcements seeking unique and innovative technologies to advance the mission of the Department.

(3) The establishment of a technical assistance team to assist in screening, as appropriate, proposals submitted to the Secretary (except as provided in subsection (c)(2)) to assess the feasibility, scientific and technical merits, and estimated cost of such proposals, as appropriate.

(4) The provision of guidance, recommendations, and technical assistance, as appropriate, to assist Federal, State, and local government and private sector efforts to evaluate and implement the use of technologies described in paragraph (1) or (2).

(5) The provision of information for persons seeking guidance on how to pursue proposals to develop or deploy technologies that would enhance homeland security, including information relating to Federal funding, regulation, or acquisition.

(c) CRITICAL INFRASTRUCTURE PROTECTION TECHNOLOGY CLEARINGHOUSE.—

(1) DESIGNATION.—Under the program required by this section, the Secretary, acting through the Under Secretary for Science and Technology, and in coordination with the Under Secretary for the National Protection and Programs Directorate, shall designate a technology clearinghouse for rapidly sharing proven technology solutions for protecting critical infrastructure.

(2) SHARING OF TECHNOLOGY SOLUTIONS.—Technology solutions shared through the clearinghouse shall draw from Government-furnished, commercially furnished, and publically available trusted sources.

(3) TECHNOLOGY METRICS.—All technologies shared through the clearinghouse shall include a set of performance and readiness metrics to assist end-users in deploying effective and timely solutions relevant for their critical infrastructures.

(4) REVIEW BY PRIVACY OFFICER.—The Privacy Officer of the Department appointed under section 222 shall annually review the clearinghouse process to evaluate its consistency with fair information practice principles issued by the Privacy Officer.

[(c)**]** *(d)* MISCELLANEOUS PROVISIONS.—

(1) IN GENERAL.—Nothing in this section shall be construed as authorizing the Secretary or the technical assistance team established under subsection (b)(3) to set standards for technology to be used by the Department, any other executive agency, any State or local government entity, or any private sector entity.

(2) CERTAIN PROPOSALS.—The technical assistance team established under subsection (b)(3) shall not consider or evaluate proposals submitted in response to a solicitation for offers for a pending procurement or for a specific agency requirement.

(3) COORDINATION.—In carrying out this section, the Secretary shall coordinate with the Technical Support Working

Group (organized under the April 1982 National Security Decision Directive Numbered 30).

* * * * * * *

SEC. 318. RESEARCH AND DEVELOPMENT STRATEGY FOR CRITICAL INFRASTRUCTURE PROTECTION.

(a) IN GENERAL.—Not later than 180 days after the date of enactment of the Critical Infrastructure Research and Development Advancement Act of 2013, the Secretary, acting through the Under Secretary for Science and Technology, shall transmit to Congress a strategic plan to guide the overall direction of Federal physical security and cybersecurity technology research and development efforts for protecting critical infrastructure, including against all threats. Once every 2 years after the initial strategic plan is transmitted to Congress under this section, the Secretary shall transmit to Congress an update of the plan.

(b) CONTENTS OF PLAN.—The strategic plan shall include the following:

(1) An identification of critical infrastructure security risks and any associated security technology gaps, that are developed following—

(A) consultation with stakeholders, including the Sector Coordinating Councils; and

(B) performance by the Department of a risk/gap analysis that considers information received in such consultations.

(2) A set of critical infrastructure security technology needs that—

(A) is prioritized based on risk and gaps identified under paragraph (1);

(B) emphasizes research and development of those technologies that need to be accelerated due to rapidly evolving threats or rapidly advancing infrastructure technology; and

(C) includes research, development, and acquisition roadmaps with clearly defined objectives, goals, and measures.

(3) An identification of laboratories, facilities, modeling, and simulation capabilities that will be required to support the research, development, demonstration, testing, evaluation, and acquisition of the security technologies described in paragraph (2).

(4) An identification of current and planned programmatic initiatives for fostering the rapid advancement and deployment of security technologies for critical infrastructure protection. The initiatives shall consider opportunities for public-private partnerships, intragovernment collaboration, university centers of excellence, and national laboratory technology transfer.

(5) A description of progress made with respect to each critical infrastructure security risk, associated security technology gap, and critical infrastructure technology need identified in the preceding strategic plan transmitted under this section.

(c) COORDINATION.—In carrying out this section, the Under Secretary for Science and Technology shall coordinate with the Under Secretary for the National Protection and Programs Directorate.

(d) CONSULTATION.—In carrying out this section, the Under Secretary for Science and Technology shall consult with—

(1) the critical infrastructure Sector Coordinating Councils;

(2) to the extent practicable, subject matter experts on critical infrastructure protection from universities, colleges, including historically black colleges and universities, Hispanic-serving institutions, and tribal colleges and universities, national laboratories, and private industry;

(3) the heads of other relevant Federal departments and agencies that conduct research and development for critical infrastructure protection; and

(4) State, local, and tribal governments as appropriate.

SEC. 319. REPORT ON PUBLIC-PRIVATE RESEARCH AND DEVELOPMENT CONSORTIUMS.

(a) IN GENERAL.—Not later than 180 days after the enactment of the Critical Infrastructure Research and Development Advancement Act of 2013, the Secretary, acting through the Under Secretary for Science and Technology, shall transmit to Congress a report on the Department's utilization of public-private research and development consortiums for accelerating technology development for critical infrastructure protection. Once every 2 years after the initial report is transmitted to Congress under this section, the Secretary shall transmit to Congress an update of the report. The report shall focus on those aspects of critical infrastructure protection that are predominately operated by the private sector and that would most benefit from rapid security technology advancement.

(b) CONTENTS OF REPORT.—The report shall include—

(1) a summary of the progress and accomplishments of ongoing consortiums for critical infrastructure security technologies;

(2) in consultation with the Sector Coordinating Councils and, to the extent practicable, in consultation with subject-matter experts on critical infrastructure protection from universities, colleges, including historically black colleges and universities, Hispanic-serving institutions, and tribal colleges and universities, national laboratories, and private industry, a prioritized list of technology development focus areas that would most benefit from a public-private research and development consortium; and

(3) based on the prioritized list developed under paragraph (2), a proposal for implementing an expanded research and development consortium program, including an assessment of feasibility and an estimate of cost, schedule, and milestones.

* * * * * * *

MICHAEL T. McCAUL, TEXAS
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER

One Hundred Thirteenth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

January 8, 2014

The Honorable Lamar Smith
Chairman
Committee on Science, Space, and Technology
2321 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Smith:

Thank you for your letter regarding H.R. 2952, the "Critical Infrastructure Research and Development Act of 2013." I acknowledge that by forgoing a sequential referral on this legislation, your Committee is not diminishing or altering its jurisdiction.

I also concur with you that forgoing action on this bill does not in any way prejudice the Committee on Science, Space, and Technology with respect to its jurisdictional prerogatives on this bill or similar legislation in the future, and I would support your effort to seek appointment of an appropriate number of conferees to any House-Senate conference involving this legislation. In addition, the Committee on Science, Space, and Technology will be added as a recipient of the report provided by the General Accountability Office, required by Section 3 of this legislation, in the final version of text voted on by the full House.

Finally, I will include your letter and this response in the report accompanying H.R. 2952 as well as the *Congressional Record* during consideration of this bill on the House floor. I appreciate your cooperation regarding this legislation, and I look forward to working with the Committee on Science, Space, and Technology as the bill moves through the legislative process.

Sincerely,

Michael T. McCaul

Michael T. McCaul
Chairman

cc: The Honorable John Boehner, Speaker
The Honorable Eric Cantor, Majority Leader
The Honorable Eddie Bernice Johnson, Ranking Member
The Honorable Bennie G. Thompson, Ranking Member
Mr. Thomas J. Wickham, Jr., Parliamentarian

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

2321 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6301

(202) 225-6371
www.science.house.gov

January 8, 2014

The Honorable Michael McCaul
Chairman
Committee on Homeland Security
H2-176
Washington, DC 20515

Dear Chairman McCaul:

I am writing to you concerning the jurisdictional interest of the Committee on Science, Space, and Technology in H.R. 2952, the "Critical Infrastructure Research and Development Advancement Act of 2013." The bill contains provisions that fall within the jurisdiction of the Committee on Science, Space, and Technology.

I recognize and appreciate the desire to bring this legislation before the House of Representatives in an expeditious manner, and accordingly, I will waive further consideration of this bill in Committee, notwithstanding any provisions that fall within the jurisdiction of the Committee on Science, Space, and Technology. This waiver, of course, is conditional on our mutual understanding that agreeing to waive consideration of this bill should not be construed as waiving, reducing, or affecting the jurisdiction of the Committee on Science, Space, and Technology.

This waiver is also given with the understanding that the Committee on Science, Space, and Technology will be added as a recipient of the report required to be provided by the General Accounting Office in Section 3 of the bill.

Additionally, the Committee on Science, Space, and Technology expressly reserves its authority to seek conferees on any provision within its jurisdiction during any House-Senate conference that may be convened on this, or any similar legislation. I ask for your commitment to support any request by the Committee for conferees on H.R. 2952 as well as any similar or related legislation.

I ask that a copy of this letter and your response be included in the report on H.R. 2952 and also be placed in the Congressional Record during consideration of this bill on the House floor.

Sincerely,

Lamar Smith

Lamar Smith
Chairman
Committee on Science,
Space, and Technology

Enclosure

cc: The Hon. John Boehner, Speaker,
The Hon. Eric Cantor, Majority Leader
The Hon. Eddie Bernice Johnson, Ranking Member, Committee on Science, Space, and Technology
The Hon. Bennie G. Thompson, Ranking Member, Committee on Homeland Security
Mr. Thomas J. Wickham, Jr., Parliamentarian

○