111TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPT. 111–486
Part 1

HOMELAND SECURITY SCIENCE AND TECHNOLOGY AUTHORIZATION ACT OF 2010

MAY 18, 2010.—Ordered to be printed

Mr. THOMPSON of Mississippi, from the Committee on Homeland Security, submitted the following

R E P O R T

[To accompany H.R. 4842]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security, to whom was referred the bill (H.R. 4842) to authorize appropriations for the Directorate of Science and Technology of the Department of Homeland Security for fiscal years 2011 and 2012, 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 "Homeland Security Science and Technology Authorization Act of 2010".

SEC. 2. TABLE OF CONTENTS.

The table of contents for this Act is as follows:

SEC. 3. DEFINITIONS.

In this Act:

(1) APPROPRIATE CONGRESSIONAL COMMITTEE.—The term "appropriate congressional committee" means the Committee on Homeland Security of the House of Representatives and any committee of the House of Representatives or the Senate having legislative jurisdiction under the rules of the House of Representatives or Senate, respectively, over the matter concerned.

(2) DEPARTMENT.—The term "Department" means the Department of Homeland Security.

(3) DIRECTORATE.—The term "Directorate" means the Directorate of Science and Technology of the Department.

(4) SECRETARY.—The term "Secretary" means the Secretary of Homeland Security.

(5) UNDER SECRETARY.—The term "Under Secretary" means the Under Secretary for Science and Technology of the Department.

SEC. 4. REFERENCES.

Except as otherwise specifically provided, whenever in this Act an amendment or repeal is expressed in terms of an amendment to, or repeal of, a provision, the reference shall be considered to be made to a provision of the Homeland Security Act of 2002 (6 U.S.C. 101 et seq.).

TITLE I—AUTHORIZATION OF APPROPRIATIONS

SEC. 101. AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated to the Under Secretary $1,121,664,000 for fiscal year 2011 and $1,155,313,920 for fiscal year 2012 for the necessary expenses of the Directorate.

TITLE II—MANAGEMENT AND ADMINISTRATION

SEC. 201. RESEARCH PRIORITIZATION AND REQUIREMENTS; PROFESSIONAL DEVELOPMENT; MILESTONES AND FEEDBACK.

(a) IN GENERAL.—Subtitle D of title II (6 U.S.C. 161 et seq.) is amended—

(1) in the subtitle heading, by striking "**Office of**";

(2) in the heading for section 231, by inserting "**OF SCIENCE AND TECHNOLOGY**" after "**OFFICE**"; and

(3) by adding at the end the following new sections:

"SEC. 238. RESEARCH PRIORITIZATION AND REQUIREMENTS.

"(a) REQUIREMENT.—The Secretary shall—

"(1) by not later than 180 days after the date of enactment of this section, establish requirements for how basic and applied homeland security research shall be identified, prioritized, funded, tasked, and evaluated by the Directorate of Science and Technology, including the roles and responsibilities of the Under Secretary for Science and Technology, the Under Secretary for Policy, the Under Secretary for Management, the Director of the Office of Risk Management and Analysis, and the heads of operational components of the Department; and

"(2) to the greatest extent possible, seek to publicize the requirements for the purpose of informing the Federal, State, and local governments, first responders, and the private sector.

"(b) CONTENTS.—In the requirements, the Secretary shall—

"(1) identify the Directorate of Science and Technology's customers within and outside of the Department;

"(2) describe the risk formula and risk assessment tools that the Department considers to identify, prioritize, and fund homeland security research projects;

"(3) describe the considerations to be used by the Directorate to task projects to research entities, including the national laboratories, federally funded research and development centers, and university-based centers;

"(4) describe the protocols to be used to assess off-the-shelf technology to determine if an identified homeland security capability gap can be addressed through the acquisition process instead of commencing research and development of technology to address that capability gap;

"(5) describe the processes to be used by the Directorate to strengthen first responder participation in identifying and prioritizing homeland security technological gaps by—

"(A) soliciting feedback from appropriate national associations and advisory groups representing the first responder community and first responders within the components of the Department;

"(B) establishing and promoting a publicly accessible portal to allow the first responder community to help the Directorate develop homeland security research and development goals; and

"(C) establishing a mechanism to publicize the Department's funded and unfunded homeland security technology priorities; and

"(6) include such other requirements, policies, and practices as the Secretary considers necessary.

"(c) ACTIVITIES IN SUPPORT OF THE RESEARCH PRIORITIZATION AND REQUIREMENTS.—Not later than one year after the date of the issuance of the requirements, the Secretary shall—

"(1) establish, through the Under Secretary for Science and Technology and Under Secretary for Management, a mandatory workforce program for the Directorate's customers in the Department to better identify and prioritize homeland security capability gaps that may be addressed by a technological solution based on the assessment required under section 239(a)(2);

"(2) establish a system to collect feedback from customers of the Directorate on the performance of the Directorate, that includes metrics for measuring customer satisfaction and the usefulness of any technology or service provided by the Directorate; and

"(3) any other activities that the Secretary considers to be necessary to implement the requirements.

"(d) QUARTERLY UPDATES ON IMPLEMENTATION.—One hundred and twenty days after the date of enactment of this section, and on a quarterly basis thereafter, the Inspector General of the Department shall submit a quarterly update to the appropriate congressional committees on the status of implementation of the research prioritization and requirements and activities in support of such requirements.

"(e) RISK ANALYSIS.—In carrying out subsection (b)(2), the Secretary shall—

"(1) submit to the appropriate congressional committees by not later than one year after the date of enactment of this subsection and annually thereafter—

"(A) a national-level risk assessment, describing and prioritizing the greatest risks to the homeland, that includes vulnerability studies, asset values (including asset values for intangible assets), estimated rates of occurrence, countermeasures employed, loss expectancy, cost/benefit analyses, and other practices generally associated with producing a comprehensive risk analysis;

"(B) an analysis of the Directorate's approach to mitigating the homeland security risks identified under subparagraph (A) through basic and applied research, development, demonstration, testing, and evaluation activities;

"(C) an analysis, based on statistics and metrics, of the effectiveness of the Directorate in reducing the homeland security risks identified under subparagraph (A) through the deployment of homeland security technologies researched or developed by the Directorate;

"(D) recommendations for how the Directorate should modify or amend its research and development activities in order to reduce the risks to the homeland identified under subparagraph (A);

"(E) a description of how the analysis required under subparagraph (A) shall be used to inform, guide, and prioritize the Department's homeland security research and development activities; and

"(F) a description of input from other relevant Federal, State, or local agencies and relevant private sector entities in conducting the risk analysis required by subparagraph (A); and

"(2) conduct research and development on ways to most effectively communicate information regarding the risks identified under paragraph (1) to the media as well as directly to the public, both on an ongoing basis and during a terrorist attack or other incident.

"(f) REPORT ON HSARPA ACTIVITIES.—

"(1) IN GENERAL.—Consistent with the Federal Acquisition Regulation and any other relevant Federal requirements, not later than 60 days after the date of enactment of this subsection and annually thereafter, the Secretary shall submit a report to the appropriate congressional committees containing the research, development, testing, evaluation, prototyping, and deployment activities undertaken by the Homeland Security Advanced Research Projects Agency during the previous fiscal year, including funds expended for such activities in the previous fiscal year.

"(2) CONTENTS.—For each activity undertaken, the report shall—

"(A) describe the corresponding risk analysis performed by the Department that supports the decision to undertake that activity; and

"(B) describe the efforts made to transition that activity into a Federal, State, or local acquisition program.

"(3) ADDITIONAL ACTIVITIES.—The Secretary shall include in each report a description of each proposal that was reviewed in the period covered by the report by the Director of the Homeland Security Advanced Research Projects Agency under section 313(d)(3), including a statement of whether the proposal received a grant, cooperative agreement, or contract from the Director.

"SEC. 239. PROFESSIONAL DEVELOPMENT.

"(a) REPORTING REQUIREMENT.—Sixty days before establishing the mandatory workforce program as required by section 238(c)(1), the Secretary shall report to the appropriate congressional committees on the following:

"(1) A description of how homeland security technological requirements are developed by the Directorate of Science and Technology's customers within the Department.

"(2) An assessment of whether Department employees receive adequate and appropriate job training to allow them to identify, express, and prioritize homeland security capability gaps.

"(3) A plan for how the Directorate, in coordination with the Domestic Nuclear Detection Office and other Department components, can enhance and improve technology requirements development and the technology acquisition process, to accelerate the delivery of effective, suitable technologies that meet performance requirements and appropriately address an identified homeland security capability gap.

"(4) An assessment of whether Congress should authorize, in addition to the program required under section 238(c)(1), a training program for Department employees to be trained in requirements writing and acquisition, that—

"(A) is prepared in consultation with the Department of Veterans Affairs Acquisition Academy and the Defense Acquisition University; and

"(B) if the Secretary determines that such additional training should be authorized by Congress, includes specification about—

"(i) the type, skill set, and job series of Department employees who would benefit from such training, including an estimate of the number of such employees;

"(ii) a suggested curriculum for the training;

"(iii) the type and skill set of educators who could most effectively teach those skills;

"(iv) the length and duration of the training;

"(v) the advantages and disadvantages of training employees in a live classroom, or virtual classroom, or both;

"(vi) cost estimates for the training; and

"(vii) the role of the Directorate in supporting the training.

"(b) USE OF RESEARCH AND DEVELOPMENT CENTER.—The Secretary is encouraged to use a federally funded research and development center to assist the Secretary in carrying out the requirements of this section.

"SEC. 240. TRACKING SYSTEMS, RESEARCH MILESTONES, AND CUSTOMER FEEDBACK.

"(a) IN GENERAL.—In establishing a system to collect feedback under section 238(c)(2), the Secretary shall—

"(1) establish a system to monitor and account for homeland security research milestones;

"(2) create a formal process for collecting feedback from customers on the effectiveness of the technology or services delivered by Directorate of Science and Technology, including through randomized sampling, focus groups, and other methods as appropriate; and

"(3) establish standards and performance measures to be met by the Directorate in order to provide high-quality customer service.

"(b) SYSTEM.—The system established under subsection (a)(1) shall identify and account for research milestones to monitor the progress of Directorate of Science and Technology research, development, testing, and evaluation activities, and collect information from the Directorate's customers about their level of satisfaction with the performance of the Directorate, including by—

"(1) allowing the Directorate to provide regular reports to its customers regarding the status and progress of research efforts of the Directorate;

"(2) collecting and evaluating customer feedback;

"(3) allowing the Secretary to evaluate how a technology or service produced as a result of the Directorate's programs has affected homeland security capability gaps; and

"(4) allowing the Secretary to report the number of products and services developed by the Directorate that have been transitioned into acquisition programs.

"(c) GUIDANCE.—The Under Secretary for Science and Technology shall publicize and implement guidance for homeland security researchers funded by the Directorate on setting valid initial and subsequent research milestones.

"(d) REPORT.—The Under Secretary shall submit a report to the appropriate congressional committees—

"(1) by not later than one year after the date of enactment of this section identifying what actions have been taken to carry out the requirements of this section; and

"(2) annually thereafter describing—

"(A) research milestones for each large project with a Federal cost share greater than $80,000,000 that has been successfully met and missed, including for each missed milestone, an explanation of why the milestone was missed; and

"(B) customer feedback collected and the success of the Directorate in meeting the customer service performance measures and standards, including an evaluation of the effectiveness of the technology or services delivered by the Directorate.".

(b) CLERICAL AMENDMENTS.—The table of contents in section 1(b) is amended in the items relating to subtitle D of title II—

(1) in the item relating to the heading for the subtitle, by striking "Office of";

(2) in the item relating to section 231, by striking "office" and inserting "Office of Science and Technology"; and

(3) by adding at the end the following new items:

"Sec. 238. Research prioritization and requirements.
"Sec. 239. Professional development.
"Sec. 240. Tracking systems, research milestones, and customer feedback.".

SEC. 202. TESTING, EVALUATION, AND STANDARDS.

Section 308 (6 U.S.C. 188) is amended by adding at the end of the following new subsection:

"(d) TEST, EVALUATION, AND STANDARDS DIVISION.—

"(1) ESTABLISHMENT.—There is established in the Directorate of Science and Technology a Test, Evaluation, and Standards Division.

"(2) DIRECTOR.—The Test, Evaluation, and Standards Division shall be headed by a Director of Test, Evaluation, and Standards, who shall be appointed by the Secretary and report to the Under Secretary for Science and Technology.

"(3) RESPONSIBILITIES, AUTHORITIES, AND FUNCTIONS.—The Director of Test, Evaluation, and Standards—

"(A) is the principal adviser to the Secretary, the Under Secretary of Management, and the Under Secretary for Science and Technology on all test and evaluation or standards activities in the Department; and

"(B) shall—

"(i) prescribe test and evaluation policies for the Department, which shall include policies to ensure that operational testing is done at facilities that already have relevant and appropriate safety and material certifications to the extent such facilities are available;

"(ii) oversee and ensure that adequate test and evaluation activities are planned and conducted by or on behalf of components of the Department in major acquisition programs of the Department, as designated by the Secretary, based on risk, acquisition level, novelty, complexity, and size of the acquisition program, or as otherwise established in statute;

"(iii) review major acquisition program test reports and test data to assess the adequacy of test and evaluation activities conducted by or on behalf of components of the Department; and

"(iv) review available test and evaluation infrastructure to determine whether the Department has adequate resources to carry out its testing and evaluation responsibilities, as established under this title.

"(4) DEPUTY DIRECTOR OF OPERATIONAL TEST AND EVALUATION.—Within the Division there shall be a Deputy Director of Operational Test and Evaluation, who—

"(A) is the principal operational test and evaluation official for the Department; and

"(B) shall—

"(i) monitor and review the operational testing and evaluation activities conducted by or on behalf of components of the Department in major acquisition programs of the Department, as designated by the Secretary, based on risk, acquisition level, novelty, complexity, and size of the acquisition program, or as otherwise established in statute;

"(ii) provide the Department with independent and objective assessments of the adequacy of testing and evaluation activities conducted in support of major acquisitions programs; and

"(iii) have prompt and full access to test and evaluation documents, data, and test results of the Department that the Deputy Director considers necessary to review in order to carry out the duties of the Deputy Director under this section.

"(5) STANDARDS EXECUTIVE.—Within this Division, there shall be a Standards Executive as described in Office of Management and Budget Circular A–119. The Standards Executive shall—

"(A) implement the Department's standards policy as described in section 102(g); and

"(B) support the development and adoption of voluntary standards in accordance with section 12(d) of the National Technology Transfer and Advancement Act of 1995 (15 U.S.C. 272 note).

"(6) LIMITATION.—The Division is not required to carry out operational testing.

"(7) EVALUATION OF DEPARTMENT OF DEFENSE TECHNOLOGIES.—The Director of Test, Evaluation, and Standards may evaluate technologies currently in use or being developed by the Department of Defense to assess whether they can be leveraged to address homeland security capability gaps.".

SEC. 203. PEER REVIEW.

(a) RESPONSIBILITIES AND AUTHORITIES OF THE UNDER SECRETARY.—Section 302 (6 U.S.C. 183) is amended by striking "and" after the semicolon at the end of paragraph (13), by striking the period at the end of paragraph (14) and inserting "; and", and by adding at the end the following new paragraph:

"(15) developing and overseeing the administration of guidelines for peer review of research and development projects, including by—

"(A) consulting with experts, including scientists and practitioners, about the research and development conducted by the Directorate of Science and Technology; and

"(B) performing ongoing independent, external, scientific peer review—

"(i) initially at the division level; or

"(ii) when divisions conduct multiple programs focused on significantly different subjects, at the program level.".

(b) REPORT.—The Secretary shall report to Congress not later than 60 days after the completion of the first review under section 302(15)(B) of the Homeland Security Act of 2002, as amended by subsection (a) of this section on—

(1) the findings of the review; and

(2) any future efforts to ensure that the Department's research projects are peer reviewed, as appropriate.

SEC. 204. OFFICE OF PUBLIC-PRIVATE PARTNERSHIPS.

(a) ESTABLISHMENT.—Section 313 (6 U.S.C. 193) is amended to read as follows:

"SEC. 313. OFFICE OF PUBLIC-PRIVATE PARTNERSHIPS.

"(a) ESTABLISHMENT OF OFFICE.—There is established an Office of Public-Private Partnerships in the Directorate of Science and Technology.

"(b) DIRECTOR.—The Office shall be headed by a Director, who shall be appointed by the Secretary. The Director shall report to the Under Secretary for Science and Technology.

"(c) RESPONSIBILITIES.—The Director, in coordination with the Private Sector Office of the Department, shall—

"(1) engage and initiate proactive outreach efforts and provide guidance on how to pursue proposals to develop or deploy homeland security technologies (including regarding Federal funding, regulation, or acquisition), including to persons associated with small businesses (as that term is defined in the Small Business Act (15 U.S.C. 631 et seq.));

"(2) coordinate with components of the Department to issue announcements seeking unique and innovative homeland security technologies to address homeland security capability gaps;

"(3) promote interaction between homeland security researchers and private sector companies in order to accelerate transition research or a prototype into a commercial product and streamline the handling of intellectual property; and

"(4) conduct technology research assessment and marketplace analysis for the purpose of identifying, leveraging, and integrating best-of-breed technologies and capabilities from industry, academia, and other Federal Government agencies, and disseminate research and findings to Federal, State, and local governments.

"(d) RAPID REVIEW DIVISION.—

"(1) ESTABLISHMENT.—There is established the Rapid Review Division within the Office of Public-Private Partnerships.

"(2) PURPOSE AND DUTIES.—

"(A) IN GENERAL.—The Division—

"(i) is responsible for maintaining a capability to perform business and technical reviews to assist in screening unsolicited homeland security technology proposals submitted to the Secretary; and

"(ii) shall assess the feasibility, scientific and technical merits, and estimated cost of such proposals.

"(B) SPECIFIC DUTIES.—In carrying out those duties, the Division shall—

"(i) maintain awareness of the technological requirements of the Directorate's customers;

"(ii) establish and publicize accessible, streamlined procedures allowing a participant to have their technology assessed by the Division;

"(iii) make knowledgeable assessments of a participant's technology after receiving a business plan, a technology proposal, and a list of corporate officers, directors, and employees with technical knowledge of the proposal, within 60 days after such a submission;

"(iv) review proposals submitted by components of the Department to the Division, subject to subsection (e); and

"(v) in reviewing proposals submitted to the Secretary, give priority to any proposal submitted by a small business concern as defined under section 3 of the Small Business Act (15 U.S.C. 632).

"(3) COORDINATION.—The Director shall submit for consideration promising homeland security technology research, development, testing, and evaluation proposals, along with any business and technical reviews, to the Director of the Homeland Security Advanced Research Projects Agency and appropriate Department components for consideration for support.

"(e) LIMITATION ON CONSIDERATION OR EVALUATION OF PROPOSALS.—The Office may not consider or evaluate homeland security technology proposals submitted in response to a solicitation for offers for a pending procurement or for a specific agency requirement.

"(f) SATELLITE OFFICES.—The Under Secretary, acting through the Director, may establish up to 3 satellite offices across the country to enhance the Department's outreach efforts. The Secretary shall notify the appropriate congressional committees in writing within 30 days after establishing any satellite office.

"(g) PERSONNEL.—The Secretary shall establish rules to prevent the Director or any other employee of the Office from acting on matters where a conflict of interest may exist.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) is amended by striking the item relating to such section and inserting the following:

"Sec. 313. Office of Public-Private Partnerships.".

(c) AUTHORIZATION OF APPROPRIATIONS.—Of the amount authorized by section 101, there is authorized to be appropriated $30,000,000 for the Office of Public-Private Partnerships for each of fiscal years 2011 and 2012.

TITLE III—REPORTS

SEC. 301. DIRECTORATE OF SCIENCE AND TECHNOLOGY STRATEGIC PLAN.

(a) IN GENERAL.—Title III (6 U.S.C. 181 et seq.) is amended by adding at the end the following new section:

"SEC. 318. STRATEGIC PLAN.

"(a) REQUIREMENT FOR STRATEGIC PLAN.—Not later than 1 year after the date of enactment of this section and every other year thereafter, the Under Secretary for Science and Technology shall prepare a strategic plan for the activities of the Directorate.

"(b) CONTENTS.—The strategic plan required by subsection (a) shall be prepared in accordance with applicable Federal requirements, and shall include the following matters:

"(1) The long-term strategic goals of the Directorate.

"(2) Identification of the research programs of the Directorate that support achievement of those strategic goals.

"(3) The connection of the activities and programs of the Directorate to requirements or homeland security capability gaps identified by customers within the Department and outside of the Department, including the first responder community.

"(4) The role of the Department's risk analysis in the activities and programs of the Directorate.

"(5) A technology transition strategy for the programs of the Directorate.

"(6) A description of the policies of the Directorate on the management, organization, and personnel of the Directorate.

"(c) SUBMISSION OF PLAN TO CONGRESS.—The Secretary shall submit to Congress any update to the strategic plan most recently prepared under subsection (a) at the same time that the President submits to Congress the budget for each even-numbered fiscal year.".

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

"Sec. 318. Strategic plan.".

SEC. 302. REPORT ON TECHNOLOGY REQUIREMENTS.

Section 302 (6 U.S.C. 182) is amended by inserting "(a) IN GENERAL.—" before the first sentence, and by adding at the end the following new subsection:

"(b) REPORT ON TECHNOLOGY REQUIREMENTS.—

"(1) IN GENERAL.—Within 90 days after the date of enactment of this subsection, and biannually thereafter, the Under Secretary shall, for each project having a Federal cost share greater than $80,000,000 that is conducted or funded by the Directorate of Science and Technology, provide to the appropriate congressional committees a list of detailed operational and technical requirements that are associated with the project.

"(2) LARGE PROJECTS.—Within 90 days after the date of enactment of this subsection, and biannually thereafter, the Secretary shall, for each project conducted or funded by a component of the Department, other than the Directorate of Science and Technology, having a life-cycle cost greater than $1,000,000,000, provide to the appropriate congressional committees detailed operational and technical requirements that are associated with the project.".

SEC. 303. REPORT ON VENTURE CAPITAL ORGANIZATION.

(a) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Secretary shall submit a report to the appropriate congressional committees—

(1) assessing the current role of the venture capital community in funding advanced homeland security technologies, including technologies proposed by small business concerns as defined under section 3 of the Small Business Act (15 U.S.C. 632); and

(2) providing recommendations about creating a nonprofit organization for the purposes of delivering advanced homeland security technologies to the homeland security community to further its missions.

(b) CONTENTS.—The report shall include the following:

(1) An assessment of the current awareness and insight that the Department has regarding advanced private sector homeland security innovation, and the Department's ability to quickly transition innovative products into acquisitions.

(2) A description of how the Department currently finds and works with emerging companies, particularly firms that have never done business with the Federal Government, small business concerns, small business concerns that are owned and operated by women, small business concerns that are owned and operated by veterans, and minority-owned and operated small business concerns.

(3) An assessment and analysis of the current role that venture capitalists play in the development of homeland security technologies, including an assessment of how the venture capital community could be leveraged to accelerate technology, foster development, and introduce new technologies needed by the homeland security community.

(4) An assessment of whether the Department could help nascent commercial technologies mature into commercial-off-the-shelf products the homeland security community could acquire.

(5) An analysis of whether the Central Intelligence Agency's In-Q-Tel organization or the Department of Defense's OnPoint Technologies organization could serve as a model for the development of homeland security technology at the Department.

(6) Recommendations of the Secretary regarding how Congress could authorize the establishment of a private, independent, not-for-profit organization to bridge the gap between the technology needs of the homeland security community and new advances in commercial technology, including specifics on potential funding levels, activities for the organization, including the provision of technical assistance, and whether to establish set-asides for small businesses that are minority-owned and operated or located in socially and economically disadvantaged areas.

(c) USE OF RESEARCH AND DEVELOPMENT CENTER.—The Secretary is encouraged to use a federally funded research and development center to produce the report under this section.

(d) AUTHORIZATION OF APPROPRIATIONS.—Of the amount authorized by section 101, there is authorized $500,000 for the report.

TITLE IV—DIRECTORATE OF SCIENCE AND TECHNOLOGY PROGRAMS

SEC. 401. LIMITATIONS ON RESEARCH.

Section 302(a)(4), as designated by section 302, is further amended by inserting after "extramural programs," the following: "that, to the greatest extent possible, addresses a prioritized risk to the homeland as identified by a risk analysis under section 226(e) of this Act".

SEC. 402. UNIVERSITY-BASED CENTERS.

(a) AUTHORIZATION OF APPROPRIATIONS.—Of the amount authorized by section 101, there is authorized to be appropriated $40,000,000 for fiscal year 2011 and $41,200,000 for fiscal year 2012 to the Secretary to carry out the university-based centers program of the Department.

(b) CRITERIA FOR DESIGNATION.—Section 308(b)(2)(B)(iii) (6 U.S.C. 188(b)(2)(B)(iii)) is amended by inserting before the period at the end the following: ", including medical readiness training and research, and community resiliency for public health and healthcare critical infrastructure".

(c) EXPLOSIVE COUNTERMEASURES OR DETECTION.—Section 308(b)(2)(B)(iv) (6 U.S.C. 188(b)(2)(B)(iv)) is amended by striking "and nuclear" and inserting "nuclear, and explosive".

SEC. 403. REVIEW OF UNIVERSITY-BASED CENTERS.

(a) GAO STUDY OF UNIVERSITY-BASED CENTERS.—Not later than 120 days after the date of enactment of this Act, the Comptroller General of the United States shall initiate a study to assess the university-based centers for homeland security program authorized by section 308(b)(2) of the Homeland Security Act of 2002 (6 U.S.C. 188(b)(2)), and provide recommendations to the appropriate congressional committees for appropriate improvements.

(b) SUBJECT MATTERS.—The study under subsection (a) shall include the following:

(1) A review of key areas of study needed to support the homeland security mission, and criteria that should be utilized to determine those key areas for which the Department should maintain, establish, or eliminate university-based centers.

(2) A review of the method by which university-based centers, federally funded research and development centers, and Department of Energy national laboratories receive tasking from the Department, including a review of how university-based research is identified, prioritized, and funded.

(3) A review of selection criteria for designating university-based centers and a weighting of such criteria.

(4) An examination of the optimal organization and role of the university-based centers in supporting the mission of the Directorate and the Department components.

(5) An identification of the most appropriate review criteria and metrics to measure demonstrable progress achieved by university-based centers in fulfilling Department taskings, and mechanisms for delivering and disseminating the research results of designated university-based centers within the Department and to other Federal, State, and local agencies.

(6) An examination of the means by which academic institutions that are not designated or associated with the designated university-based centers can optimally contribute to the research mission of the Directorate.

(7) An assessment of the interrelationship between the different university-based centers.

(8) A review of any other essential elements of the programs determined in the conduct of the study.

(c) MORATORIUM ON NEW UNIVERSITY-BASED CENTERS.—The Secretary may not designate any new university-based centers to research new areas in homeland security prior to the completion of the Comptroller General's review.

SEC. 404. CYBERSECURITY RESEARCH AND DEVELOPMENT.

(a) IN GENERAL.—The Under Secretary shall support research, development, testing, evaluation, and transition of cybersecurity technology, including fundamental, long-term research to improve the ability of the United States to prevent, protect against, detect, respond to, and recover from acts of terrorism and cyber attacks, with an emphasis on research and development relevant to large-scale, high-impact attacks.

(b) ACTIVITIES.—The research and development supported under subsection (a) shall include work to—

(1) advance the development and accelerate the deployment of more secure versions of fundamental Internet protocols and architectures, including for the domain name system and routing protocols;

(2) improve and create technologies for detecting attacks or intrusions, including real-time monitoring and real-time analytic technologies;

(3) improve and create mitigation and recovery methodologies, including techniques and policies for real-time containment of attacks, and development of resilient networks and systems that degrade gracefully;

(4) develop and support infrastructure and tools to support cybersecurity research and development efforts, including modeling, testbeds, and data sets for assessment of new cybersecurity technologies;

(5) assist the development and support of technologies to reduce vulnerabilities in process control systems;

(6) develop and support cyber forensics and attack attribution; and

(7) test, evaluate, and facilitate the transfer of technologies associated with the engineering of less vulnerable software and securing the information technology software development lifecycle.

(c) COORDINATION.—In carrying out this section, the Under Secretary shall coordinate activities with—

(1) the Under Secretary for National Protection and Programs; and

(2) the heads of other relevant Federal departments and agencies, including the National Science Foundation, the Defense Advanced Research Projects Agency, the Information Assurance Directorate of the National Security Agency, the National Institute of Standards and Technology, the Department of Commerce, and other appropriate working groups established by the President to identify unmet needs and cooperatively support activities, as appropriate.

(d) AUTHORIZATION OF CYBERSECURITY PREPAREDNESS CONSORTIUM AND TRAINING CENTER.—

(1) CYBERSECURITY PREPAREDNESS CONSORTIUM.—Subtitle C of title II of the Homeland Security Act of 2002 (6 U.S.C. 121 et seq.) is amended by adding at the end the following new section:

"SEC. 226. CYBERSECURITY PREPAREDNESS CONSORTIUM.

"(a) IN GENERAL.—To assist the Secretary in carrying out the requirements of section 404(a) of the Homeland Security Science and Technology Authorization Act of 2010, the Secretary may establish a consortium to be known as the 'Cybersecurity Preparedness Consortium'.

"(b) FUNCTIONS.—The Consortium shall—

"(1) provide training to State and local first responders and officials specifically for preparing and responding to cybersecurity attacks;

"(2) develop and update a curriculum and training model for State and local first responders and officials;

"(3) provide technical assistance services to build and sustain capabilities in support of cybersecurity preparedness and response;

"(4) conduct cybersecurity training and simulation exercises to defend from and respond to cyber attacks; and

"(5) coordinate all cybersecurity preparedness training activities conducted by the Department.

"(c) MEMBERS.—The Consortium shall consist of academic, nonprofit, and government partners that—

"(1) have demonstrated expertise in developing and delivering cybersecurity training in support of homeland security;

"(2) have demonstrated ability to utilize existing courses and expertise developed by the Department;

"(3) have demonstrated ability to coordinate with the National Domestic Preparedness Consortium and other training programs within the Department; and

"(4) include at least 3 academic institutions that are any combination of historically Black colleges and universities, Hispanic-serving institutions, or Tribal Colleges and Universities, that fulfill the criteria of paragraphs (1), (2) and (3) of this subsection.

"(d) DEFINITIONS.—In this section:

"(1) HISTORICALLY BLACK COLLEGE OR UNIVERSITY.—The term 'historically Black college or university' has the meaning given the term 'part B institution' in section 322(2) of the Higher Education Act of 1965 (20 U.S.C. 1061(2)).

"(2) HISPANIC-SERVING INSTITUTION.—The term 'Hispanic-serving institution' has the meaning given that term in section 502 of the Higher Education Act of 1965 (20 U.S.C. 1101(a)).

"(3) TRIBAL COLLEGE OR UNIVERSITY.—The term 'Tribal College or University' has the meaning given that term in section 316(b) of the Higher Education Act of 1965 (20 U.S.C. 1059c(b)).".

(2) CLERICAL AMENDMENT.—Section 1(b) of such Act is further amended by adding at the end of the items relating to such subtitle the following new item:

"Sec. 226. Cybersecurity Preparedness Consortium.".

(3) CYBERSECURITY TRAINING CENTER.—Subtitle C of title II of the Homeland Security Act of 2002 (6 U.S.C. 121 et seq.) is further amended by adding at the end the following new section:

"SEC. 227. CYBERSECURITY TRAINING CENTER.

"The Secretary may establish where appropriate a Cybersecurity Training Center to provide training courses and other resources for State and local first responders and officials to improve preparedness and response capabilities.".

(4) CLERICAL AMENDMENT.—Section 1(b) of such Act is further amended by adding at the end of the items relating to such subtitle the following new item:

"Sec. 227. Cybersecurity Training Center.".

(e) AUTHORIZATION OF APPROPRIATIONS.—Of the amount authorized by section 101, there is authorized to be appropriated $75,000,000 to the Department for each of fiscal years 2011 and 2012 for the cybersecurity research and development activities of the Directorate to prevent, detect, and respond to acts of terrorism and other large-scale disruptions to information infrastructure.

SEC. 405. NATIONAL RESEARCH COUNCIL STUDY OF CYBERSECURITY INCENTIVES.

(a) STUDY.—Not later than 90 days after the date of enactment of this Act, the Under Secretary and the Under Secretary for National Protection and Programs of the Department shall seek to enter into an agreement with the National Research Council of the National Academy of Sciences to conduct a study to assess methods that might be used to promote market mechanisms that further cybersecurity and make recommendations for appropriate improvements thereto.

(b) SUBJECT MATTERS.—The study required under subsection (a) shall include the following:

(1) Liability that subjects software and system vendors and system operators to potential damages for system breaches.

(2) Mandated reporting of security breaches that could threaten critical functions, including provision of electricity and resiliency of the financial sector.

(3) Regulation that under threat of civil penalty, imposes best practices on system operators of critical infrastructure.

(4) Certification from standards bodies about conformance to relevant cybersecurity standards that can be used as a marketplace differentiation.

(5) Accounting practices that require companies to report their cybersecurity practices and postures and the results of independently conducted red team simulated attacks or exercises.

(6) Cybersecurity risk insurance, including analysis of the current marketplace and recommendations to promote cybersecurity insurance.

(c) SUBMISSION TO CONGRESS.—Not later than two years after the date of enactment of this Act, the Secretary shall submit to the appropriate congressional committees the results of the study required under subsection (a), together with any recommendations of the Secretary related thereto.

(d) AUTHORIZATION OF APPROPRIATIONS.—Of the amount authorized by section 101, there is authorized to be appropriated $500,000 to the Department for fiscal year 2011 to carry out this section.

SEC. 406. RESEARCH ON CYBER COMPROMISE OF INFRASTRUCTURE.

(a) IN GENERAL.—Pursuant to section 201 of the Homeland Security Act of 2002 (6 U.S.C. 121) and in furtherance of domestic preparedness for and collective response to a cyber attack by a terrorist or other person, the Secretary, working with the heads of other national security and intelligence agencies, shall conduct research and determine if the security of federally owned programmable electronic devices and communication networks, including hardware, software, and data, essential to the reliable operation of critical electric infrastructure has been compromised.

(b) SCOPE OF RESEARCH.—The scope of the research required under subsection (a) shall include the following:

(1) The extent of any compromise.

(2) An identification of any attackers, including any affiliations with terrorists, terrorist organizations, state entities, and non-state entities.

(3) The method of penetration.

(4) Ramifications of any such compromise on future operations of critical electric infrastructure.

(5) Secondary ramifications of any such compromise on other critical infrastructure sectors and the functioning of civil society.

(6) Ramifications of any such compromise on national security, including war fighting capability.

(7) Recommended mitigation activities.

(c) REPORT.—Not later than 30 days after the date a determination has been made under subsection (a), the Secretary shall submit to the appropriate congressional committees a report on the findings of such determination. The report may contain a classified annex if the Secretary determines it to be appropriate.

SEC. 407. DUAL-USE TERRORIST RISKS FROM SYNTHETIC GENOMICS.

(a) SENSE OF CONGRESS.—It is the sense of Congress that the field of synthetic genomics has the potential to facilitate enormous gains in fundamental discovery and biotechnological applications, but it also has inherent dual-use homeland security risks that must be managed.

(b) REQUIREMENT.—The Under Secretary shall examine and report to the appropriate congressional committees by not later than one year after the date of enactment of this Act on the homeland security implications of the dual-use nature of synthetic genomics and, if the Under Secretary determines that such research is appropriate, may conduct research in that area, including—

(1) determining the current capability of synthetic nucleic acid providers to effectively differentiate a legitimate customer from a potential terrorist or other malicious actor;

(2) determining the current capability of synthetic nucleic acid providers to effectively screen orders for sequences of homeland security concern; and

(3) making recommendations regarding screening software, protocols, and other remaining capability gaps uncovered by the study.

SEC. 408. UNDERWATER TUNNEL SECURITY DEMONSTRATION PROJECT.

(a) IN GENERAL.—The Under Secretary, in consultation with the Assistant Secretary of the Transportation Security Administration, shall conduct a demonstration project to test and assess the feasibility and effectiveness of certain technologies to enhance the security of underwater public transportation tunnels against terrorist attacks involving the use of improvised explosive devices.

(b) INFLATABLE PLUGS.—At least one of the technologies tested under subsection (a) shall be inflatable plugs that may be rapidly deployed to prevent flooding of an underwater public transportation tunnel.

(c) REPORT.—Not later than 180 days after the completion of the demonstration project under subsection (a), the Under Secretary shall submit to the appropriate congressional committees a report on the results of the demonstration project.

SEC. 409. THREATS RESEARCH AND DEVELOPMENT.

(a) IN GENERAL.—The Under Secretary, in carrying out responsibilities under section 302 of the Homeland Security Act of 2002 (6 U.S.C. 182), may support research, development, testing, evaluation, and transition of technology that increases the Nation's preparedness against chemical and biological threats and strengthens the Nation's preparedness and collective response against those threats through improved threat awareness and advanced surveillance, detection, and protective countermeasures, and to enhance the development of border security technology.

(b) BIOLOGICAL SECURITY.—To carry out subsection (a), the Under Secretary may conduct research to develop understanding, technologies, and systems needed to protect against biological attacks on the Nation's population or infrastructure, including—

(1) providing advanced planning tools, concepts of operations (including alarm resolution protocols), and training exercises for responding to and recovering from biological attacks;

(2) developing biological assays and improved detection technology that will operate with faster detection times, lower costs, and the potential for increased geographical coverage to the Nation when compared to existing homeland security technologies;

(3) characterizing threats posed by biological weapons, anticipating future threats, conducting comprehensive threat and risk assessments to guide prioritization of the Nation's biodefense investments, and developing population threat assessments that inform the issuance of material threat determinations;

(4) conducting bioforensics research in support of criminal investigations to aid attribution, apprehension, and prosecution of a terrorist or other perpetrator of a biological attack, and providing tools and facilities that Federal law enforcement investigators need to analyze biological threat evidence recovered, including operation of the National Bioforensic Analysis Center; and

(5) conducting appropriate research and studies that will increase our understanding of and uncertainties associated with risk and threats posed by biological agents through the Biological Threat Characterization Center and other means as determined by the Secretary.

(c) AGRICULTURAL SECURITY.—The Under Secretary may conduct research and development to enhance the protection of the Nation's agriculture and food system against terrorist attacks, and other emergency events through enhancement of current agricultural countermeasures, development of new agricultural countermeasures, and provision of safe, secure, state-of-the-art biocontainment laboratories for researching foreign animal and zoonotic diseases, including—

(1) developing technologies to defend the Nation against the natural and intentional introduction of selected foreign animal diseases, developing next-generation vaccines and diagnostics in coordination with the Department of Agriculture, and modeling the spread of foreign animal diseases and their economic impact to evaluate strategies for controlling outbreaks; and

(2) leading the Department effort to enhance interagency coordination of research and development of agricultural disease countermeasures.

(d) CHEMICAL SECURITY.—The Under Secretary may develop technology to reduce the Nation's vulnerability to chemical warfare agents and commonly used toxic industrial chemicals, including—

(1) developing a robust and enduring analytical capability in support of chemical countermeasures development, including developing and validating forensic methodologies and analytical tools, conducting risk and vulnerability assessments based on chemical threat properties, and maintaining infrastructure including the Chemical Security Analysis Center;

(2) developing technology to detect a chemical threat release; and

(3) developing technologies and guidance documents to foster a coordinated approach to returning a chemically contaminated area to a normal condition, and to foster analysis of contaminated areas both before and after the restoration process.

(e) RISK ASSESSMENTS.—

(1) IN GENERAL.—The Under Secretary shall produce risk assessments for biological and chemical threats, and shall coordinate with the Director of the Domestic Nuclear Detection Office of the Department, the Assistant Secretary of the Office of Health Affairs of the Department, and the Assistant Secretary of Infrastructure Protection of the Department on an integrated risk assessment, including regarding chemical, biological, radiological, nuclear, and explosive threats.

(2) USAGE.—The assessments required under paragraph (1) shall be used to inform and guide the threat assessments and determinations by the Secretary of Homeland Security regarding agents and toxins pursuant to section 302(9) of the Homeland Security Act of 2002 (6 U.S.C. 182(9)), and to guide prioritization of other homeland defense activities, as appropriate.

(3) TASK FORCE.—The Under Secretary for Science and Technology shall convene an interagency task force of relevant subject matter experts to assess the proposed methodology to be used for each assessment required under paragraph (1), and to provide recommendations to the Under Secretary as to the adequacy of such methodology.

(f) BORDER SECURITY.—The Under Secretary may develop technology, in coordination with the Commissioner of Customs and Border Protection, to gain effective control of the international land borders of the United States within 5 years after the date of enactment of this Act. In carrying out such development activities, the Under Secretary shall ensure coordination and integration between new technologies developed and those already utilized by U.S. Customs and Border Protection.

SEC. 410. MARITIME DOMAIN AWARENESS AND MARITIME SECURITY TECHNOLOGY TEST, EVALUATION, AND TRANSITION CAPABILITIES.

(a) GLOBAL MARITIME DOMAIN AWARENESS AND MARITIME SECURITY TECHNOLOGY TEST, EVALUATION, AND TRANSITION CAPABILITIES.—

(1) ESTABLISHMENT.—The Secretary shall establish capabilities for conducting global maritime domain awareness and maritime security technology test, evaluation, and transition, as provided in this subsection.

(2) PURPOSE.—The purpose of such capabilities shall be to—

(A) direct technology test, evaluation, and transition activities in furtherance of border and maritime security; and

(B) evaluate such technology in diverse environments including coastal, seaport, and offshore locations.

(b) COORDINATION.—The Secretary, acting through the Under Secretary, shall ensure that—

(1) technology test, evaluation, and transition efforts funded by the Department in furtherance of border and maritime security avoid duplication of efforts, reduce unnecessary redundancies, streamline processes, increase efficiencies, and otherwise complement existing Department and other efforts in border and maritime security; and

(2) the results of such efforts are shared with the appropriate congressional committees and others as determined appropriate by the Secretary.

SEC. 411. RAPID BIOLOGICAL THREAT DETECTION AND IDENTIFICATION.

(a) IN GENERAL.—Notwithstanding section 302(4) of the Homeland Security Act of 2002 (6 U.S.C. 182(4)), the Secretary shall require the Under Secretary, in consultation with other relevant operational components of the Department, to assess whether the development of screening capabilities for pandemic influenza and other infectious diseases should be undertaken by the Directorate to support entry and exit screening at ports of entry and for other purposes.

(b) DEVELOPMENT OF METHODS.—If the Under Secretary determines that the development of such screening capabilities should be undertaken, the Secretary shall, to the extent possible, initiate development of safe and effective methods to rapidly screen incoming travelers at ports of entry for pandemic influenza and other infectious diseases.

(c) COLLABORATION.—In developing methods under subsection (b), the Secretary may collaborate with other Federal agencies, as appropriate.

SEC. 412. EDUCATING THE PUBLIC ABOUT RADIOLOGICAL THREATS.

(a) PUBLIC AWARENESS CAMPAIGN.—The Secretary shall develop a public awareness campaign to enhance preparedness and collective response to a radiological attack, including the following:

(1) A clear explanation of the dangers associated with radioactive materials.

(2) Possible effects of different levels of radiation exposure, including a clear description of the how radiation exposure occurs and the amount of exposure necessary to be of concern.

(3) Actions that members of the public should take regarding evacuation, personal decontamination, and medical treatment.

(b) RECOVERY.—The Secretary shall develop a plan for postevent recovery from a radiological attack. Such plan shall include the following:

(1) A definition of the demarcation between response and recovery from a radiological attack.

(2) Consideration of multiple attack scenarios, including a worst-case scenario.

(3) Consideration of multiple recovery strategies, including decontamination, demolition and removal, and relocation.

(4) Consideration of economic, health, and psychological effects.

SEC. 413. RURAL RESILIENCE INITIATIVE.

(a) IN GENERAL.—The Under Secretary shall conduct research intended to assist State, local, and tribal leaders and the private sector in developing the tools and methods to enhance preparation for, and response and resilience to, terrorist events and other incidents.

(b) INCLUDED ACTIVITIES.—Activities under this section may include—

(1) research and implementation through outreach activities with rural communities;

(2) an examination of how communities employ resilience capabilities and response assets;

(3) a community resilience baseline template for determining the resilience capacity of a rural community;

(4) a plan to address community needs for resilience;

(5) an education program for community leaders and first responders about their resilience capacity and mechanisms for mitigation, including via distance learning; and

(6) a mechanism by which this research can serve as a model for adoption by communities across the Nation.

SEC. 414. SENSE OF CONGRESS REGARDING THE NEED FOR INTEROPERABILITY STANDARDS FOR INTERNET PROTOCOL VIDEO SURVEILLANCE TECHNOLOGY.

It is the sense of Congress that—

(1) video surveillance systems that operate over the Internet are an emerging homeland security technology that has the potential of significantly improving homeland security forensic and analytical capability;

(2) to realize the full security benefits of such emerging homeland security technology, there should be interoperability standards for such technology;

(3) the Directorate, working with other appropriate Federal agencies, should encourage the private sector to develop interoperability standards for such emerging homeland security technology; and

(4) such efforts will help the Federal Government, which is one of the largest users of surveillance technology, in detecting, deterring, preventing, and responding to terrorist attacks.

SEC. 415. HOMELAND SECURITY SCIENCE AND TECHNOLOGY FELLOWS PROGRAM.

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

"SEC. 319. HOMELAND SECURITY SCIENCE AND TECHNOLOGY FELLOWS PROGRAM.

"(a) ESTABLISHMENT.—The Secretary, acting through the Under Secretary for Science and Technology, shall establish a fellows program, to be known as the Homeland Security Science and Technology Fellows Program, under which the Under Secretary shall facilitate the temporary placement of scientists in relevant scientific or technological fields for up to two years in components of the Department with a need for scientific and technological expertise.

"(b) UTILIZATION OF FELLOWS.—

"(1) IN GENERAL.—Under the Program, the Under Secretary may employ fellows—

"(A) for the use of the Directorate of Science and Technology; or

"(B) for the use of Department components outside the Directorate, under an agreement with the head of such a component under which the component will reimburse the Directorate for the costs of such employment.

"(2) RESPONSIBILITIES.—Under such an agreement—

"(A) the Under Secretary shall—

"(i) solicit and accept applications from individuals who are currently enrolled in or who are graduates of post-graduate programs in scientific and engineering fields related to the promotion of securing the homeland, including—

"(I) biological, chemical, physical, behavioral, social, health, medical, and computational sciences;

"(II) geosciences;

"(III) all fields of engineering; and

"(IV) such other disciplines as are determined relevant by the Secretary;

"(ii) screen applicant candidates and interview them as appropriate to ensure that they possess the appropriate level of scientific and engineering expertise and qualifications;

"(iii) provide a list of qualified applicants to the heads of Department components seeking to utilize qualified fellows;

"(iv) pay financial compensation to such fellows;

"(v) coordinate with the Chief Security Officer to facilitate and expedite provision of security clearances to fellows, as appropriate; and

"(vi) otherwise administer all aspects of the fellows' employment with the Department; and

"(B) the head of the component utilizing the fellow shall—

"(i) select a fellow from the list of qualified applicants provided by the Under Secretary;

"(ii) reimburse the Under Secretary for the costs of employing the fellow selected; and

"(iii) be responsible for the day-to-day management of the fellow.

"(c) APPLICATIONS FROM ASSOCIATIONS.—The Under Secretary may accept applications under subsection (b)(2)(A) that are submitted by science or policy associations on behalf of individuals whom such an association has determined may be qualified applicants under the program.".

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

"Sec. 319. Homeland Security Science and Technology Fellows Program.".

SEC. 416. BIOLOGICAL THREAT AGENT ASSAY EQUIVALENCY.

(a) IN GENERAL.—Title III (6 U.S.C. 181 et seq.) is further amended by adding at the end the following new section:

"SEC. 320. BIOLOGICAL THREAT AGENT ASSAY EQUIVALENCY PROGRAM.

"(a) IN GENERAL.—To facilitate equivalent biological threat agent identification among federally operated biomonitoring programs, the Under Secretary, in consulta-

tion with the Director of the Centers for Disease Control and Prevention, may implement an assay equivalency program for biological threat assays.

"(b) FEATURES.—In order to establish assay performance equivalency to support homeland security and public health security decisions, the program may—

"(1) evaluate biological threat detection assays, their protocols for use, and their associated response algorithms for confirmation of biological threat agents, taking performance measures and concepts of operation into consideration; and

"(2) develop assay equivalency standards based on the findings of the evaluation under paragraph (1).

"(c) UPDATE.—The Under Secretary shall update the program as necessary.

"(d) IMPLEMENTATION.—The Secretary shall—

"(1) require implementation of the standards developed under subsection (b)(2) for all Department biomonitoring programs; and

"(2) make such standards available to support all other Federal biomonitoring programs.

"(e) ASSAY DEFINED.—In this section the term 'assay' means any scientific test that is—

"(1) designed to detect the presence of a biological threat agent; and

"(2) of a type selected under criteria established by the Secretary.".

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

"Sec. 320. Biological threat agent assay equivalency program.".

SEC. 417. STUDY OF FEASIBILITY AND BENEFIT OF EXPANDING OR ESTABLISHING PROGRAM TO CREATE A NEW CYBERSECURITY CAPACITY BUILDING TRACK AT CERTAIN INSTITUTIONS OF HIGHER EDUCATION.

(a) IN GENERAL.—Within 90 days of enactment, the Secretary, in coordination with the National Science Foundation, shall commission a study by a nonprofit research institution to determine the feasibility and potential benefit of expanding the Federal Cyber Service Scholarship for Service Program, or establishing a parallel program, as methods to create a new cybersecurity or information assurance capacity building track at institutions of higher education that are not currently designated as a National Center of Academic Excellence in Information Assurance Education or a National Center of Academic Excellence in Research.

(b) SUBJECT MATTERS.—The study under subsection (a) shall include examinations of the following:

(1) The feasibility and potential benefit of allowing the following types of institutions into the existing Federal Cyber Service program:

(A) Community colleges.

(B) Institutions offering an undergraduate degree, graduate degree, or post-graduate degree, but do not qualify under the existing program.

(C) Institutions offering a certificate or industry-recognized credential.

(2) The feasibility and potential benefit of establishing a new program modeled after the Federal Cyber Service program to build capacity at—

(A) community colleges;

(B) institutions offering an undergraduate degree, graduate degree, or post-graduate degree, but do not qualify under the existing program; or

(C) institutions offering a certificate or industry-recognized credential.

(3) The projected extent to which an expansion of the existing Federal Cyber Service program as described in paragraph (1) would—

(A) expand the availability of qualified individuals to work in information assurance and cybersecurity within the Department and other Federal, State, local, and tribal agencies, and the private sector;

(B) encourage institutions of higher education to develop a new information assurance or cybersecurity education undergraduate degree programs, graduate degree programs, or programs conferring a certificate or industry-recognized credential;

(C) increase the number of students graduating annually from existing information assurance or cybersecurity education undergraduate degree programs, graduate degree programs, or programs conferring a certificate or industry-recognized credential; or

(D) improve existing information assurance or cybersecurity education undergraduate degree programs, graduate degree programs, or programs conferring a certificate or industry-recognized credential.

(4) The projected extent to which the establishment of a new program modeled after the Federal Cyber Service program as described in paragraph (2) would—

(A) expand the availability of qualified individuals to work in information assurance and cybersecurity within the Department and other Federal, State, local, and tribal agencies, and the private sector;

(B) encourage institutions of higher education to develop a new information assurance or cybersecurity education undergraduate degree programs, graduate degree programs, or programs conferring a certificate or industry-recognized credential;

(C) increase the number of students graduating annually from existing information assurance or cybersecurity education undergraduate degree programs, graduate degree programs, or programs conferring a certificate or industry-recognized credential; or

(D) improve existing information assurance or cybersecurity education undergraduate degree programs, graduate degree programs, or programs conferring a certificate or industry-recognized credential.

(c) REPORT.—Not later than 30 days after receiving the findings of the study, the Secretary shall transmit the findings, together with any comments thereon by the Secretary, to the appropriate congressional committees.

SEC. 418. SENSE OF CONGRESS REGARDING CENTERS OF EXCELLENCE.

It is the sense of Congress that centers of excellence have the potential—

(1) to be a very useful tool in developing defensive countermeasures to secure critical infrastructure and prevent terrorism; and

(2) to play a key role in the Department's efforts to research and develop new technologies to secure the homeland.

SEC. 419. ASSESSMENT, RESEARCH, TESTING, AND EVALUATION OF TECHNOLOGIES TO MITIGATE THE THREAT OF SMALL VESSEL ATTACK.

The Under Secretary may—

(1) assess what technologies are available to mitigate the threat of small vessel attack in secure zones of ports, including the use of transponders or radio frequency identification devices to track small vessels; and

(2) conduct research, testing, and evaluation of new technologies that might be capable of tracking small vessels.

SEC. 420. RESEARCH AND DEVELOPMENT PROJECTS.

Section 831 (6 U.S.C. 391) is amended—

(1) in subsection (a), by striking "2010," and inserting "2012,";

(2) in subsection (a), by adding at the end the following new paragraph:

"(3) PRIOR APPROVAL.—In any case in which the Under Secretary for Science and Technology intends to exercise other transaction authority, the Under Secretary must receive prior approval from the Secretary after submitting to the Secretary a proposal that includes the rationale for why a grant or contract issued in accordance with the Federal Acquisition Regulation is not feasible or appropriate and the amount to be expended for such project. In such a case, the authority for evaluating the proposal may not be delegated by the Secretary to anyone other than the Under Secretary for Management."; and

(3) by redesignating subsection (e) as subsection (i), and by inserting after subsection (d) the following new subsections:

"(e) ANNUAL REPORT ON EXERCISE OF OTHER TRANSACTION AUTHORITY.—

"(1) IN GENERAL.—The Secretary shall submit to the appropriate congressional committees an annual report on the exercise of other transaction authority.

"(2) CONTENT.—The report shall include the following:

"(A) The subject areas in which research projects were conducted using other transaction authority.

"(B) The extent of cost-sharing for such projects among Federal and non-Federal sources.

"(C) The extent to which use of other transaction authority has addressed a homeland security capability gap identified by the Department of Homeland Security.

"(D) The total amount of payments, if any, that were received by the Federal Government as a result of such exercise of other transaction authority during the period covered by the report.

"(E) The rationale for using other transaction authority, including why grants or contracts issued in accordance with the Federal Acquisition Regulation were not feasible or appropriate.

"(F) the amount expended for each such project.

"(f) TRAINING.—The Secretary shall develop a training program for acquisitions staff in the use of other transaction authority to help ensure the appropriate use of such authority.

"(g) REVIEW AUTHORITY.—The exercise of other transaction authority shall be subject to review by the Comptroller General of the United States to ensure that an agency is not attempting to avoid the requirements of procurement statutes and regulations.

"(h) OTHER TRANSACTION AUTHORITY DEFINED.—In this section the term 'other transaction authority' means authority under subsection (a).".

SEC. 421. NATIONAL URBAN SECURITY TECHNOLOGY LABORATORY.

(a) IN GENERAL.—The National Urban Security Technology Laboratory (formerly the Environmental Measurements Laboratory) is authorized within the Directorate for fiscal years 2011 and 2012.

(b) RESPONSIBILITIES.—The Under Secretary shall utilize the National Urban Security Technology Laboratory to test, evaluate, and analyze homeland security capabilities and serve as a technical authority to first responders and State and local entities, including by—

(1) conducting test programs, pilots projects, demonstrations, and other forms of evaluations of homeland security technologies both in the field and in the laboratory;

(2) applying knowledge of operational end-user environments and support for operational integration to technology development, including—

(A) training;

(B) exercises;

(C) equipment;

(D) tactics;

(E) techniques; and

(F) procedures;

(3) representing interests and requirements between technology developers and operational end-users; and

(4) supporting development and use of homeland security equipment and operational standards.

TITLE V—DOMESTIC NUCLEAR DETECTION OFFICE

SEC. 501. AUTHORIZATION OF APPROPRIATIONS.

There is authorized to be appropriated for the Domestic Nuclear Detection Office of the Department—

(1) $305,840,000 for fiscal year 2011; and

(2) $315,005,000 for fiscal year 2012.

SEC. 502. DOMESTIC NUCLEAR DETECTION OFFICE OVERSIGHT.

(a) SENSE OF CONGRESS.—It is the sense of Congress that the Directorate should conduct basic and innovative research and nondevelopmental testing on behalf of the Domestic Nuclear Detection Office (in this section referred to as "DNDO"), in order to advance next generation nuclear detection technologies.

(b) INTERNAL REVIEW OF PROJECT SELECTION AND EVALUATION METHODOLOGY.—Not later than 90 days after the date of enactment of this Act, the Director of the DNDO shall begin an internal review of the methodology by which research, development, testing, and evaluation is identified, prioritized, and funded by the DNDO. In conducting such review, the Director shall consult with the Under Secretary and the heads of all operational components of the Department that own, operate, or maintain nuclear or radiological detection technologies.

(c) CONTENTS OF REVIEW.—In carrying out the review under subsection (b), the Director of the DNDO shall—

(1) identify the process by which basic and applied research and operational testing that should be conducted in concert and under agreement with the Directorate;

(2) describe the roles, responsibilities, common definitions, standard operating procedures, and decision process for research, development, testing, and evaluation activities;

(3) describe and implement a transparent system for tracking research, development, testing, and evaluation requirements;

(4) describe and implement a mechanism to provide regular updates to components of the Department on the progress of such research;

(5) evaluate the degree to which needs of the operational components of the Department and State and local first responders are being adequately addressed by the existing project selection process, and if not, how such process can be improved;

(6) establish a method to collect and evaluate Department component feedback;

(7) utilize departmental matrices and systems to determine if technologies produced by the Directorate have enhanced the ability of Department components to perform their missions;

(8) identify appropriate five-year levels of investment in basic and applied research and development, in particular among the Department laboratories, federally funded research and development centers, university-based centers, Department of Energy national laboratories, and other Federal laboratories;

(9) project balance of use of the entities referred to in paragraph (8) among the Directorate and other Department components; and

(10) establish a formal merit review process, with external peer review where appropriate.

(d) REPORT.—Not later than one year after the completion of the review required by subsection (b), the Director of the DNDO shall submit to the Secretary and the appropriate congressional committees a report containing the findings of such review, together with information on the systems, methods, and mechanisms established, and recommendations for additional improvements.

(e) UPDATES ON IMPLEMENTATION.—One hundred and twenty days after the date of enactment of this Act, and annually thereafter, the Inspector General of the Department shall submit to the appropriate congressional committees an update on the status of implementation of this section and activities in support of such implementation.

SEC. 503. STRATEGIC PLAN AND FUNDING ALLOCATIONS FOR GLOBAL NUCLEAR DETECTION ARCHITECTURE.

Not later than 180 days after the date of enactment of this Act, the Secretary shall submit to the appropriate congressional committees a report containing the following:

(1) A strategic plan for the global nuclear detection architecture to deter and detect the transport of nuclear or radioactive materials by all means possible, with specific focus on establishing the goals, objectives, and cost projections for the next five years, including a discussion of—

(A) technological and nontechnological methods to increase detection capabilities;

(B) the preventive nature of the global nuclear detection architecture, including projected impact on would-be terrorists;

(C) detection capability enhancements for the various transportation modes, at ports of entry and between ports of entry;

(D) balanced risk-based deployment of detection assets across all border and other pathways; and

(E) any emerging threat vectors identified by the Director of the Domestic Nuclear Detection Office.

(2) In consultation with the Secretary of Defense, the Secretary of Energy, the Secretary of State, the Nuclear Regulatory Commission, the Intelligence Community, and the Attorney General, an analysis of overall budget allocations that determines whether Governmentwide nuclear detection resources clearly align with identified priorities to maximize results and minimize duplication of efforts.

SEC. 504. RADIATION PORTAL MONITOR ALTERNATIVES.

(a) SENSE OF CONGRESS.—It is the sense of Congress that in view of the Secretary's decision not to certify advanced spectroscopic portal monitors for primary screening applications because they do not offer a significant increase in operational effectiveness over existing technology, the Director must attempt to identify viable alternatives.

(b) ANALYSIS AND REPORT.—The Director of the Domestic Nuclear Detection Office shall analyze and report to the appropriate congressional committees by not later than 90 days after the date of enactment of this Act on both existing and developmental alternatives to existing radiation portal monitors and advanced spectroscopic portal monitors that would provide the Department with a significant increase in operational effectiveness for primary screening for radioactive materials.

SEC. 505. AUTHORIZATION OF SECURING THE CITIES INITIATIVE.

(a) FINDINGS.—Congress finds the following:

(1) The Securing the Cities Initiative of the Department uses next generation radiation detection technology to detect the transport of nuclear and radiological material in urban areas by terrorists or other unauthorized individuals.

(2) The technology used by partners in the Securing the Cities Initiative leverages radiation detection technology used at ports of entry.

(3) The Securing the Cities Initiative has fostered unprecedented collaboration and coordination among its Federal, State, and local partners.

(4) The Securing the Cities Initiative is a critical national capability to detect the dangerous introduction of nuclear and radiological material.

(b) AUTHORIZATION OF APPROPRIATIONS.—Of amounts authorized by section 501, there is authorized to be appropriated to the Director of the Domestic Nuclear Detection Office of the Department for the Securing the Cities Initiative such sums as may be necessary for each of fiscal years 2011 and 2012, including—

(1) for each city in which it has been implemented by fiscal year 2009—

(A) $20,000,000 for fiscal year 2011; and

(B) $10,000,000 for fiscal year 2012; and

(2) for additional Securing the Cities initiatives to be implemented in not fewer than 2 sites participating in the Urban Area Security Initiative, such sums as may be necessary each fiscal year to implement and sustain each additional initiative.

TITLE VI—CLARIFYING AMENDMENTS

SEC. 601. FEDERALLY FUNDED RESEARCH AND DEVELOPMENT CENTERS.

Section 305 (6 U.S.C. 184) is amended—

(1) by inserting "(a) ESTABLISHMENT.—" before the first sentence; and

(2) by adding at the end the following new subsections:

"(b) CONGRESSIONAL TASKING.—Upon a request of the chairman and the ranking minority member of an appropriate congressional committee, a federally funded research and development center established under this section may perform independent analysis of homeland security issues and report its findings to the appropriate congressional committees and the Secretary.

"(c) CONGRESSIONAL OVERSIGHT.—Federally funded research and development centers established under this section are encouraged, upon request of the chairman and the ranking minority member of an appropriate congressional committee, to provide to the committee a copy of any report it produces for the Department or any of its components.

"(d) CONFLICTS OF INTEREST.—The Secretary shall review and revise, as appropriate, the policies of the Department relating to personnel conflicts of interest to ensure that such policies specifically address employees of federally funded research and development centers established under this section who are in a position to make or materially influence research findings or agency decisionmaking.

"(e) ANNUAL REPORTS.—Each federally funded research and development center established under this section shall transmit to the Secretary and appropriate congressional committees an annual report on the activities of the center.".

SEC. 602. ELIMINATION OF HOMELAND SECURITY INSTITUTE.

(a) REPEAL.—Section 312 (6 U.S.C. 192) is repealed.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) is amended by striking the item relating to such section.

SEC. 603. GAO STUDY OF THE IMPLEMENTATION OF THE STATUTORY RELATIONSHIP BETWEEN THE DEPARTMENT AND THE DEPARTMENT OF ENERGY NATIONAL LABORATORIES.

(a) IN GENERAL.—Not later than 120 days after the date of the enactment of this Act, the Comptroller General of the United States shall—

(1) conduct a study to assess the implementation of the statutory relationship between the Department and the Department of Energy national laboratories, as established by section 309(a)(2) of the Homeland Security Act of 2002 (6 U.S.C. 189(a)(2)); and

(2) submit recommendations to the appropriate congressional committees for appropriate improvements to such relationship.

(b) STUDY SUBJECTS.—The study shall include the following:

(1) Review of how the Department and the Department of Energy national laboratories—

(A) communicate needs and capabilities; and

(B) select projects to be performed by the Department of Energy national laboratories under such statutory relationship.

(2) Review of contracting mechanisms that the Department and the Department of Energy national laboratories use to initiate and track work under such statutory relationship.

(3) Review of the fraction of Department of Energy national laboratory work performed for the Department under such statutory relationship, compared to

other Department of Energy national laboratory work performed for the Department on a "work for others" basis.

(4) Review of the cost savings to the Department and the Department of Energy achieved through use of such statutory relationship, compared to other Department of Energy national laboratory work performed for the Department on a "work for others" basis.

TITLE VII—COMMISSION ON THE PROTECTION OF CRITICAL ELECTRIC AND ELECTRONIC INFRASTRUCTURES

SEC. 701. COMMISSION ON THE PROTECTION OF CRITICAL ELECTRIC AND ELECTRONIC INFRASTRUCTURES.

(a) ESTABLISHMENT.—There is established the Commission on the Protection of Critical Electric and Electronic Infrastructures (in this section referred to as the "Commission").

(b) PURPOSES.—

(1) IN GENERAL.—The purposes of the Commission are to—

(A) assess vulnerabilities of electric and electronic infrastructures, including—

(i) all components of the United States electric grid, including electricity generation, transmission, distribution and metering; and

(ii) all computerized control systems used in all United States critical infrastructure sectors;

(B) provide a clear and comprehensive strategy and specific recommendations for protecting these critical electric and electronic infrastructures; and

(C) test, evaluate, and report on specific mitigation protection and recovery devices or methods.

(2) IN PARTICULAR.—The Commission shall give particular attention to threats that can disrupt or damage critical electric and electronic infrastructures, including—

(A) cyber attacks or unintentional cyber disruption;

(B) electromagnetic phenomena such as geomagnetically induced currents, intentional electromagnetic interference, and electromagnetic pulses caused by nuclear weapons; and

(C) other physical attack, act of nature, or accident.

(c) COMPOSITION OF COMMISSION.—

(1) MEMBERS.—The Commission shall be composed of 9 members, of whom—

(A) 1 member shall be appointed by the Chairman of the House of Representatives Committee on Homeland Security;

(B) 1 member shall be appointed by the ranking minority member of the House of Representatives Committee on Homeland Security;

(C) 1 member shall be appointed by the Chairman of the House of Representatives Committee on Energy and Commerce;

(D) 1 member shall be appointed by the ranking minority member of the House of Representatives Committee on Energy and Commerce;

(E) 1 member shall be appointed by the Chairman of the Senate Committee on Homeland Security and Governmental Affairs;

(F) 1 member shall be appointed by the ranking minority member of the Senate Committee on Homeland Security and Governmental Affairs;

(G) 1 member shall be appointed by the Chairman of the Senate Committee on Energy and Natural Resources;

(H) 1 member shall be appointed by the ranking minority member of the Senate Committee on Energy and Natural Resources; and

(I) 1 member who shall serve as the Chairman of the Commission, and who shall be appointed by the Speaker of the House of Representatives with the concurrence of the President Pro Tempore of the Senate.

(2) QUALIFICATIONS.—It is the sense of Congress that individuals appointed to the Commission should be United States citizens, with significant depth of experience in electric and electronic infrastructures, their function, and their protection, as well as the threats to these infrastructures as identified in subsection (b)(2).

(3) DEADLINE FOR APPOINTMENT.—All members of the Commission shall be appointed within 30 days after the date of enactment of this Act.

(4) INITIAL MEETING.—The Commission shall meet and begin the operations of the Commission as soon as practicable.

(5) QUORUM; VACANCIES.—After its initial meeting, the Commission shall meet upon the call of the Chairman or a majority of its members. Six members of the Commission shall constitute a quorum. Any vacancy in the Commission shall not affect its powers, but shall be filled in the same manner in which the original appointment was made.

(d) RESPONSIBILITIES OF COMMISSION.—The Commission shall address—

(1) the quantification of the threats identified in subsection (b)(2) to the United States electric and electronic infrastructure, and a cost-benefit analysis of possible protection and recovery strategies;

(2) the roles, missions, and structure of all relevant Federal, State, and local government departments and agencies with responsibilities for ensuring protection and reliability for electric and electronic infrastructures;

(3) the roles, missions, and structure of all relevant private sector entities with responsibilities for ensuring protection and reliability for electric and electronic infrastructures;

(4) inter-agency coordination between and among the entities identified in paragraphs (2) and (3); and

(5) recommendations for protections and recovery devices and measures.

(e) POWERS OF COMMISSION.—

(1) HEARINGS AND EVIDENCE.—The Commission or, on the authority of the Commission, any subcommittee or member thereof, may, for the purpose of carrying out this section, hold such hearings and sit and act at such times and places, take such testimony, receive such evidence, and administer such oaths as the Commission or such designated subcommittee or designated member may determine advisable.

(2) CONTRACTING.—The Commission may, to such extent and in such amounts as are provided in appropriations Acts, enter into contracts to enable the Commission to discharge its duties under this subtitle.

(3) STAFF OF COMMISSION.—

(A) APPOINTMENT AND COMPENSATION.—The Chairman of the Commission, in accordance with rules agreed upon by the Commission, may appoint and fix the compensation of a staff director and such other personnel as may be necessary to enable the Commission to carry out its functions, without regard to the provisions of title 5, United States Code, governing appointments in the competitive service, and without regard to the provisions of chapter 51 and subchapter III of chapter 53 of such title relating to classification and General Schedule pay rates, except that no rate of pay fixed under this subsection may exceed the equivalent of that payable for a position at level I of the Executive Schedule under section 5316 of title 5, United States Code.

(B) PERSONNEL AS FEDERAL EMPLOYEES.—

(i) IN GENERAL.—The executive director and any employees of the Commission shall be employees under section 2105 of title 5, United States Code, for purposes of chapters 63, 81, 83, 84, 85, 87, 89, and 90 of that title.

(ii) MEMBERS OF COMMISSION.—Subparagraph (A) shall not be construed to apply to members of the Commission.

(C) DETAILEES.—Any Federal Government employee may be detailed to the Commission without reimbursement from the Commission, and such detailee shall retain the rights, status, and privileges of his or her regular employment without interruption.

(D) CONSULTANT SERVICES.—The Commission may procure the services of experts and consultants in accordance with section 3109 of title 5, United States Code, but at rates not to exceed the daily rate paid a person occupying a position at level I of the Executive Schedule under section 5315 of title 5, United States Code.

(E) SECURITY CLEARANCES.—The Chairman shall place an emphasis on hiring and retaining employees, contractors, and detailees with active security clearances. For employees who do not have security clearances but are determined by the Chairman to need them, the Central Intelligence Agency, Department of Energy, Department of Defense, and any other relevant agency shall expedite the necessary clearance processes.

(F) FORMER EMP COMMISSION STAFF AND RESOURCES.—The Chairman may make use of any existing and viable staff and resources previously employed by the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack established by section 1401 of Public Law 106–398 (114 Stat. 1654A–345).

(4) INFORMATION FROM FEDERAL AGENCIES.—

(A) IN GENERAL.—The Commission may secure directly from any executive department, bureau, agency, board, commission, office, independent establishment, or instrumentality of the Government, information, suggestions, estimates, and statistics for the purposes of this section. Each department, bureau, agency, board, commission, office, independent establishment, or instrumentality shall, to the extent authorized by law, furnish such information, suggestions, estimates, and statistics directly to the Commission, upon request made by the Chairman, the chairman of any subcommittee created by a majority of the Commission, or any member designated by a majority of the Commission.

(B) RECEIPT, HANDLING, STORAGE, AND DISSEMINATION.—Information shall only be received, handled, stored, and disseminated by members of the Commission and its staff consistent with all applicable statutes, regulations, and Executive orders.

(5) ASSISTANCE FROM FEDERAL AGENCIES.—

(A) GENERAL SERVICES ADMINISTRATION.—The Administrator of General Services shall provide to the Commission on a reimbursable basis and as necessary, administrative support and other services for the performance of the Commission's functions.

(B) OTHER DEPARTMENTS AND AGENCIES.—In addition to the assistance prescribed in paragraph (1), departments and agencies of the United States may provide to the Commission such services, funds, facilities, staff, and other support services as they may determine advisable and as may be authorized by law.

(6) GIFTS.—The Commission may accept, use, and dispose of gifts or donations of services or property.

(7) POSTAL SERVICES.—The Commission may use the United States mails in the same manner and under the same conditions as departments and agencies of the United States.

(f) PUBLIC MEETINGS AND RELEASE OF PUBLIC VERSIONS OF REPORTS.—The Commission shall—

(1) hold public hearings and meetings to the extent appropriate;

(2) release public versions of the report required under subsection (g); and

(3) conduct any public hearing in a manner consistent with the protection of sensitive or classified information provided to or developed for or by the Commission as required by any applicable statute, regulation, or Executive order.

(g) REPORT.—Not later than 180 days after the appointment of the Commission, and annually thereafter, the Commission shall submit to the President and Congress a report containing such findings, conclusions, and recommendations for protection and recovery measures for electric and electronic infrastructures as have been agreed to by a majority of Commission members.

(h) FUNDING.—Of the amounts authorized by section 101, there is authorized to be appropriated for the activities of the Commission under this section—

(1) $4,000,000 for fiscal year 2011; and

(2) $4,000,000 for fiscal year 2012.

PURPOSE AND SUMMARY

The purpose of H.R. 4842 is to authorize the Directorate of Science and Technology of the Department of Homeland Security for fiscal years 2011 and 2012.

BACKGROUND AND NEED FOR LEGISLATION

Congress authorized the Science and Technology Directorate in the Homeland Security Act of 2002. The Domestic Nuclear Detection Office was authorized by the Security and Accountability For Every Port Act of 2006. Over the years, the Committee on Homeland Security has considered measures affecting both components, but has never passed a comprehensive, multi-year authorization like H.R. 4842.

In March 2009, on a bipartisan basis, the Committee on Homeland Security began a review of the activities of the Department's Science and Technology Directorate and Domestic Nuclear Detection Office. The Homeland Security Act broadly authorizes the

Under Secretary for Science and Technology to conduct research, development, testing, and evaluation activities for the Department, utilizing national laboratories and federally funded research and development centers, and specifically transfers a number of functions to the Under Secretary for the purposes of achieving his or her responsibilities. In reviewing the Department's use of these authorities, the Committee determined that accountability and internal procedures, essential to the Department's ability to perform its research and development mission, were insufficient.

The Homeland Security Science and Technology Authorization Act of 2010 addresses management, administration, and programmatic areas affecting the Science and Technology Directorate ("S&T") and the Domestic Nuclear Detection Office ("DNDO"). The legislation principally emphasizes management and administrative aspects. To foster a culture that puts the needs of S&T's customers at the forefront, and more closely align research and development activities with identified homeland security risks, the legislation directs the establishment of a more rigorous process within the S&T Directorate for identifying, prioritizing, and funding research opportunities. The legislation places a number of additional reporting requirements on the Department to ensure compliance with the law and Congressional intent. The legislation contains several specific programmatic areas for research.

HEARINGS

No specific legislative hearing was held on H.R. 4842, though the Committee did hold related oversight hearings.

On March 3, 2010, the Committee's Subcommittee on Emerging Threats, Cybersecurity, Science and Technology held an oversight hearing entitled "The Department of Homeland Security's Science and Technology Directorate." The Subcommittee received testimony from Dr. Tara O'Toole, Under Secretary for Science and Technology at the Department of Homeland Security. During the hearing, Under Secretary O'Toole expressed support for concepts contained within the Committee's legislation.

On July 21, 2009, the Committee's Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology held a hearing entitled "Securing the Modern Electric Grid from Physical and Cyber Attacks." The Subcommittee received testimony from Dr. William Graham, Chair, Commission to Assess the Threat to the United States from Electromagnetic Pulse; Mr. Mark Fabro, President and Chief Security Scientist, Lofty Perch; Mr. Michael Assante, Chief Security Officer, North American Electric Reliability Corporation; Mr. Steve Naumann, Vice President of Wholesale Markets, Representing Edison Electric Institute and Electric Power Supply Association; Mr. Joe McClelland, Director of Reliability, Federal Energy Regulatory Commission; Ms. Patricia Hoffman, Acting Assistant Secretary, Office of Electricity Delivery and Energy Reliability; Mr. Sean McGurk, Director, Control Systems Security Program, Department of Homeland Security; and Ms. Cita Furlani, Director, Information Technology Laboratory, National Institute of Standards and Technology.

On June 9, 2009, the Committee's Subcommittee on Emerging Threats, Cybersecurity, Science and Technology held an oversight hearing entitled "The FY 2010 Budget for the Directorate for

Science & Technology, the Office of Health Affairs, and the Domestic Nuclear Detection Office." The Subcommittee received testimony from Mr. Brad Buswell, Acting Under Secretary for Science and Technology, Chuck Gallaway, Acting Director of the Domestic Nuclear Detection Office, and Dr. John Krohmer, Acting Assistant Secretary and Chief Medical Officer, Office of Health Affairs. The testimony of these individuals helped establish the Committee's legislative priorities for the Science and Technology Directorate and the Domestic Nuclear Detection Office.

COMMITTEE CONSIDERATION

On March 16, 2010, the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology considered H.R. 4842 and ordered the measure to be forwarded to the Full Committee for consideration, with the recommendation that it be adopted, by voice vote.

The Subcommittee took the following actions:

The Subcommittee adopted H.R. 4842, as amended, by voice vote. The following amendments were offered:

An amendment offered by MR. AUSTRIA to H.R. 4842, (#1), In section 402—(1) before the text insert "(a) Authorization of Appropriations.—"; and (2) add at the end the following new subsection entitled "(b) Criteria for Designation."; was AGREED TO by voice vote.

An amendment offered by MS. KILROY to H.R. 4842, (#2), In section 404(b), strike "and" after the semicolon at the end of paragraph (5), and insert after paragraph (5) the following new paragraph (and redesignate accordingly): (6) develop and support cyber forensics and attack attribution; and; was AGREED TO by voice vote.

An amendment offered by MS. SANCHEZ to H.R. 4842, (#3), In section 405(b)(2), strike "critical societal functions" and insert "critical functions, including provisions of electricity and resiliency of the financial sector". In section 405(b)(6) before the period insert ", including analysis of the current marketplace and recommendations to promote cybersecurity insurance".; was AGREED TO by voice vote.

An amendment offered by MR. LUJÁN to H.R. 4842, (#4), At the end of title IV add a new section entitled "Sec. __. GAO Study of the Implementation of the special statutory relationship between the Department and the Department of Energy National Laboratories."; was AGREED TO by voice vote.

The Committee on Homeland Security considered H.R. 4842 on April 15, 2010, and ordered H.R. 4842 to be favorably reported to the House, as amended, by a recorded vote of 26 yeas and 0 nays (Roll Call Vote No. 23).

The Committee adopted H.R. 4842, as amended, by voice vote.

The following amendments were offered:

An Amendment in the Nature of a Substitute offered by MR. THOMPSON to H.R. 4842, (#1); was AGREED TO by voice vote. A unanimous consent request to adopt amendments numbered #1A through #1P, as amended, where applicable, was agreed to.

An Amendment offered by MS. TITUS to the Amendment in the Nature of a Substitute to H.R. 4842, (#1A); Page 16, line 24, before the semicolon insert ", which shall include policies to ensure that operational testing is done at facilities that already have relevant and appropriate safety and material certifications to the extent such facilities are available."; was AGREED TO by unanimous consent.

An Amendment offered by MR. CAO to the Amendment in the Nature of a Substitute to H.R. 4842, (#1B); At the end of title IV add a new section entitled "Sec. __. Homeland Security Science and Technology Fellows Program."; was AGREED TO by unanimous consent.

An Amendment offered by MR. OWENS to the Amendment in the Nature of a Substitute to H.R. 4842, (#1C); Page 23, strike "and" after the semicolon at line 5, strike the period at line 8 and insert "and", and after line 8 and insert a new clause: (v) in reviewing proposals submitted to the Secretary, shall give priority to any proposal submitted by a small business concern as defined under section 3 of the Small Business Act (15 U.S.C. 632).; was AGREED TO by unanimous consent.

An Amendment offered by MR. OLSON to the Amendment in the Nature of a Substitute to H.R. 4842, (#1D); At the end of title IV add a new section entitled "Sec. __ Biological Threat Agent Assay Equivalency."; was AGREED TO by unanimous consent.

An Amendment offered by MS. KIRKPATRICK to the Amendment in the Nature of a Substitute to H.R. 4842, (#1E); At the end of title IV add a new section entitled "Sec. __. Study of Feasibility and Benefit of Expanding or Establishing Program to Create a New Cybersecurity Capacity Building Track at Certain Institutions of Higher Education."; was AGREED TO by unanimous consent.

An Amendment offered by MR. SOUDER to the Amendment in the Nature of a Substitute to H.R. 4842, (#1F); Section 409 is amended with the following: Page 40, line 10—strike the "." and insert " , and to enhance the development of border security technology." and by adding a new subsection entitled "(f) Border Security."; was AGREED TO by unanimous consent.

An Amendment offered by MS. HARMAN to the Amendment in the Nature of a Substitute to H.R. 4842, (#1G); At the end of title IV add a new section entitled "Sec. __. Sense of Congress Regarding Centers of Excellence."; was AGREED TO by unanimous consent.

An Amendment offered by MS. HARMAN to the Amendment in the Nature of a Substitute to H.R. 4842, (#1H); At the end of title IV add a new section entitled "Sec. __. Assessment, Research, Testing, and Evaluation of Technologies to Mitigate the Threat of Small Vessel Attack."; was AGREED TO by unanimous consent.

An Amendment offered by MR. MCCAUL to the Amendment in the Nature of a Substitute to H.R. 4842, (#1I); In Section 404 "Cybersecurity and Research and Development", insert a new subsection (d) entitled "Authorization of Cyber-

security Preparedness Consortium and Training Center."; was AGREED TO, as amended, by unanimous consent.

An Amendment offered by MS. JACKSON LEE to the Amendment offered by MR. MCCAUL (#1I) to the Amendment in the Nature of a Substitute to H.R. 4842, (#1I1); In proposed section 226(c), in paragraph (3) after "Department" strike the period and insert ": and" and after paragraph (3) insert a new paragraph (4) At the end of the proposed section 226, add a new subsection entitled "(d) Definitions."; was AGREED TO by unanimous consent.

An Amendment offered by MR. MCCAUL to the Amendment in the Nature of a Substitute to H.R. 4842, (#1J); At the end of title IV add a new section entitled "Sec. __. Research and Development Projects."; was AGREED TO by unanimous consent.

An Amendment offered by MR. MCCAUL to the Amendment in the Nature of a Substitute to H.R. 4842, (#1K); At the end of title II, section 202, insert a new section entitled "(7) Evaluation of Department of Defense Technologies".; was AGREED TO by unanimous consent.

An Amendment offered by MS. CLARKE to the Amendment in the Nature of a Substitute to H.R. 4842, (#1L); At the end of title IV add a new section entitled "Sec. __. National Urban Security Technology Laboratory."; was AGREED TO by unanimous consent.

An Amendment offered by MS. JACKSON LEE to the Amendment in the Nature of a Substitute to H.R. 4842, (#1M); Page 21, line 4, before "provide" insert "engage and initiate proactive outreach efforts and".; was AGREED TO by unanimous consent.

An Amendment offered by MS. JACKSON LEE to the Amendment in the Nature of a Substitute to H.R. 4842, (#1N); Page 37, strike line 17 and insert the following: (2) An identification of any attackers, including any affiliations with terrorists, terrorist organizations, state entities and non-state entities.; was AGREED TO by unanimous consent.

An Amendment offered by MS. JACKSON LEE to the Amendment in the Nature of a Substitute to H.R. 4842, (#1O); Page 33, beginning at line 17, strike "including monitoring technologies" and insert "including real-time monitoring and real-time analytic technologies"; Page 33, line 20, strike "for" and insert "and policies for real-time" after "techniques for"; Page 33, line 21, insert a comma after "attacks".; was AGREED TO by unanimous consent.

An Amendment offered by MR. CUELLAR to the Amendment in the Nature of a Substitute to H.R. 4842, (#1P); Page 13, line 19, strike the period and insert "including through randomized sampling, focus groups, and other methods as appropriate.". Page 13, strike "and" after the semicolon at line 15, strike the period at line 19 and insert "; and", and after line 19 insert the following new paragraph: "(3) establish standards and performance measures to be met by the Directorate in order to provide high-quality customer service." Page 15, line 10, after "collected" insert "and the success of the Directorate in meeting the customer service perform-

ance and standards".; was AGREED TO by unanimous consent.

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.

The Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology considered H.R. 4842 on March 16, 2010, no recorded votes were requested during the Subcommittee consideration.

The Full Committee considered H.R. 4842 on April 15, 2010. The following recorded vote was requested:

H.R. 4842, to authorize appropriations for the Directorate of Science and Technology of the Department of Homeland Security for fiscal years 2011 and 2012, and for other purposes., was ordered to be favorably reported to the House, as amended, by a recorded vote of 26 yeas and 0 nays (Roll Call Vote No. 23).

The vote was as follows:

YEAS	NAYS
MR. THOMPSON	
MS. SANCHEZ	
MR. CUELLAR	
MR. CARNEY	
MS. CLARKE	
MS. RICHARDSON	
MRS. KIRKPATRICK	
MR. LUJÁN	
MR. OWENS	
MR. PASCRELL	
MR. CLEAVER	
MR. GREEN	
MR. HIMES	
MS. KILROY	
MS. TITUS	
MR. KING	
MR. SMITH	
MS. SOUDER	
MR. LUNGREN	
MR. ROGERS	
MR. MCCAUL	
MR. DENT	
MR. BILIRAKIS	
MR. OLSON	
MR. CAO	
MR. AUSTRIA	

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.

In March 2009, on a bipartisan basis, the Committee on Homeland Security began conducting a review of the activities of the De-

partment of Homeland Security's ("Department" or "DHS") Science and Technology Directorate ("S&T") and the Domestic Nuclear Detection Office ("DNDO"). The Committee engaged the homeland security research and development community—including small, medium, and large companies, national laboratories, "think-tanks", and other interested parties—in a series of meetings designed to provide stakeholders an opportunity to provide the Committee feedback about the existing structure of the Science and Technology Directorate and the Domestic Nuclear Detection Office and propose recommendations for improvement. The Committee received extensive feedback from these meetings, and incorporated many of the findings from those discussions into the legislation.

Since the inception of the Science and Technology Directorate, many observers—including Congress—have been critical of its performance. In fact, for the first several years of its existence, the Directorate was criticized for being a "hobby shop," working on technological fixes that were not obviously tied into the mission of the Department. In 2006, Admiral Jay Cohen was appointed Under Secretary, promising to change the culture and project selection methodology. Under Secretary Cohen enjoyed some success according to a recent comprehensive review of the Directorate by the National Academy of Public Administration (NAPA): "S&T has made strides towards becoming a mature and productive research and development organization, particularly during the last three years." However, NAPA found that despite these advancements, the Directorate's ability to fulfill its mission is "limited by the lack of a cohesive strategy, the insularity that defines its culture, and the lack of mechanisms necessary to assess its performance in a systematic way."

In performing a year-long review of the Directorate, the Committee found that while it has become more responsive to the needs of Department components—its primary customers—when it comes to funding research, the Directorate lacks a robust methodology to determine what projects to fund, how much to fund, how to transition them into acquisition programs, and how to evaluate their effectiveness. Further, the Directorate is unable to provide specific evidence that DHS-funded research is being transitioned into technologies for operators to use, that operators are satisfied with the technology or service that the Directorate provides, or that DHS-funded projects are effectively reducing security risks to the homeland.

S&T research activities have indeed led to improved security of the Nation. In response to Committee questions, the Directorate points to a number of technologies, products, and services that it has delivered since 2003; many of these items are being used by customers from DHS, the first responder community, and infrastructure owners and operators. While the Directorate should be commended for these activities, it must do more to create robust processes to ensure the effectiveness and usefulness of the technologies it creates.

The Committee believes that requiring S&T to establish management and administration processes will enhance the long-term productivity and effectiveness of the Directorate.

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. 4842, the Homeland Security Science and Technology Authorization Act of 2010, 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, May 3, 2010.

Hon. BENNIE G. THOMPSON,
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. 4842, the Homeland Security Science and Technology Authorization Act of 2010.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Mark Grabowicz, who can be reached at 226–2860.

Sincerely,

DOUGLAS W. ELMENDORF.

Enclosure.

H.R. 4842—Homeland Security Science and Technology Authorization Act of 2010

Summary: H.R. 4842 would authorize the appropriation of about $1.1 billion for fiscal year 2011 and about $1.2 billion for 2012 for the Directorate of Science and Technology in the Department of Homeland Security (DHS). The bill also would authorize the appropriation of about $306 million for 2011 and $315 million for 2012 for the Domestic Nuclear Detection Office in DHS. Assuming appropriation of the authorized amounts, CBO estimates that implementing the bill would cost $2.9 billion over the 2011–2015 period.

In addition, H.R. 4842 would establish a Commission on the Protection of Critical Electric and Electronic Infrastructures. Because the bill would authorize the commission to accept and use gifts, enacting the legislation could have a negligible impact on offsetting receipts and associated direct spending. Therefore, pay-as-you-go procedures would apply to the legislation. Enacting H.R. 4842 would not affect revenues.

H.R. 4842 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would impose no costs on state, local, or tribal governments.

Estimated cost to the Federal Government: The estimated budgetary impact of H.R. 4842 is shown in the following table. The costs of this legislation fall within budget function 750 (administration of justice). CBO assumes that the amounts authorized will be ap-

propriated by the start of each fiscal year and that outlays will follow the historical rate of spending for the authorized activities.

	By fiscal year, in millions of dollars—					
	2011	2012	2013	2014	2015	2011–2015
CHANGES IN SPENDING SUBJECT TO APPROPRIATION						
Authorization Level	1,428	1,470	0	0	0	2,898
Estimated Outlays	554	959	885	500	0	2,898

Pay-as-you-go considerations: The Statutory Pay-As-You-Go Act of 2010 establishes budget reporting and enforcement procedures for legislation affecting direct spending or revenues. The net changes in outlays that are subject to those pay-as-you-go procedures are shown in the following table. (Enacting the bill would not affect revenues.)

CBO ESTIMATE OF PAY-AS-YOU-GO EFFECTS FOR H.R. 4842, THE HOMELAND SECURITY SCIENCE AND TECHNOLOGY AUTHORIZATION ACT OF 2010, AS ORDERED REPORTED BY THE HOUSE COMMITTEE ON HOMELAND SECURITY ON APRIL 15, 2010

	By fiscal year, in millions of dollars												
	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2010–2015	2010–2020
NET INCREASE OR DECREASE (−) IN THE DEFICIT													
Statutory Pay-As-You-Go Impact	0	0	0	0	0	0	0	0	0	0	0	0	0

Intergovernmental and private-sector impact: H.R. 4842 contains no intergovernmental mandates as defined in UMRA and would impose no costs on state, local, or tribal governments.

Estimate prepared by: Federal Costs: Mark Grabowicz; Impact on State, Local, and Tribal Governments: Melissa Merrell; Impact on the Private Sector: Paige Piper/Bach.

Estimate 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. 4842 contains the following general performance goals, and objectives, including outcome related goals and objectives authorized.

H.R. 4842 authorizes the activities of the Department of Homeland Security's Science and Technology Directorate and the Domestic Nuclear Detection Office for Fiscal Years 2011 and 2012. H.R. 4842 authorizes overall appropriations levels for the two entities, sets requirements for management and administration, risk analysis, research, development, testing and evaluation activities, and reporting to Congress. In addition, H.R. 4842 authorizes certain specific programs of particular interest to Congress and authorizes a new Congressional Commission to assist Congress and the Department in protecting our critical infrastructure.

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.

ADVISORY COMMITTEE STATEMENT

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

CONSTITUTIONAL AUTHORITY STATEMENT

Pursuant to clause 3(d)(1) of rule XIII of the Rules of the House of Representatives, the Committee finds that the Constitutional authority for this legislation is provided in Article I, section 8, clause 1, which grants Congress the power to provide for the common Defense of the United States.

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

Sec. 1. Short Title.
"Homeland Security Science and Technology Authorization Act of 2010."

Sec. 2. Table of Contents.

Sec. 3. Definitions.
Defines "appropriate congressional committee" as "Committee on Homeland Security of the House of Representatives and any committee of the House of Representatives or the Senate having legislative jurisdiction under the rules of the House of Representatives or the Senate, respectively, over the matters concerned"; "Department"; "Directorate"; "Secretary"; and "Under Secretary."

Sec. 4. References.
States that the Homeland Security Act of 2002 is the Act that is being amended by this legislation unless otherwise noted.

TITLE I—AUTHORIZATION OF APPROPRIATIONS

Sec. 101. Authorization of Appropriations.
Authorizes appropriations of $1,121,664,000 for fiscal year 2011, and $1,155,313,920 for fiscal year 2012 for the Science and Technology Directorate.

TITLE II—MANAGEMENT AND ADMINISTRATION

Sec. 201. Research Prioritization and Requirements; Professional Development; Milestones and Feedback.

This section requires the Secretary, within 180 days of enactment, to establish requirements for how basic and applied homeland security research is identified, prioritized, funded, tasked, and evaluated by Science and Technology Directorate ("S&T"), including relative roles and responsibilities of high-level Department of Homeland Security ("Department" or "DHS") officials.

The requirements shall: identify S&T customers; describe the Department's risk assessment tools used to prioritize and fund research projects; describe project tasking methodology used by the Directorate; describe protocols to assess commercial technology prior to conducting new research; and detail first responder participation including through a publicly accessible portal.

Not later than one year after issuing the requirements, the Secretary is required to establish a mandatory workforce program to help S&T customers better identify and prioritize homeland security capability gaps and a system to collect performance feedback from customers.

Starting 120 days after enactment, the Inspector General of the Department of Homeland Security is required to submit quarterly updates on the status of the requirements and the implementation of activities in support of the requirements.

To inform these requirements, this section also requires the Secretary to: (1) submit to Congress an annual prioritized assessment of homeland risks, S&T's approach to mitigating those risks, and whether S&T's products have helped reduce those risks; and (2) to conduct research on how to most effectively communicate risk information to the media as well as directly to the public, both on an ongoing basis and during times of emergency.

This section also requires an annual report on the research, development, testing, evaluation, prototyping, and deployment activities of the Homeland Security Advanced Research Projects Agency for the previous year, including how those activities are tied to risk.

Sixty days prior to establishing the mandatory workforce program to enhance S&T customers' ability to identify and prioritize homeland security capability gaps, the Secretary is required to report to Congress on how technological capability requirements are developed within the Department, whether there is adequate job training within the Department for this activity, how S&T can enhance technology requirements development, and whether Congress should authorize an additional training program for this activity. If training is required, the section requires the Secretary to specify which Departmental employees would benefit, a suggested curriculum, projected costs for the program, and other details. The Secretary is encouraged to use a federally funded research and development center to carry out requirements of the section to enhance professional development.

This section also requires the Secretary to establish a system to monitor and account for homeland security research milestones, create a formal process for collecting feedback from customers on the effectiveness of the product delivered by S&T, and establish standards and performance measures to be met by S&T to provide high-quality service to its customers.

The Secretary must issue guidance to homeland security researchers funded by S&T on setting research milestones.

Under this section, the Under Secretary must submit an annual report describing the actions taken to achieve the goals of this section, including information on the extent to which research milestones for each Department-funded research project costing at least $80,000,000 are met.

The Committee believes that the Department should make its decisions based on risk, whenever possible. The requirement for an annual, prioritized risk analysis, a key element not only of this section but also called for in the Quadrennial Homeland Security Review, is intended to provide a basis for the Secretary's decisions regarding resource allocation, operational activities, and technology development.

The Committee believes that a well-informed, engaged, and resilient public increases our homeland security. To that end, the Committee directs the Under Secretary to research and develop how best to communicate homeland security information to the public.

The Committee strongly believes that for S&T to succeed in meeting the homeland security technology needs of the Department, there must be a cadre of personnel at the Department with the capacity to appropriately define requirements. The Committee intends to help bolster capacity throughout the Department by requiring the Secretary to provide mandatory training to the DHS workforce.

This section also requires the Directorate to describe the processes used by S&T to strengthen first responder participation in identifying and prioritizing homeland security technological gaps. The Committee believes that the TechSolutions Program, an S&T program that allows the emergency response community to identify mission capability gaps that can be addressed by S&T through information, resources, and technology solutions, meets the requirements of this subsection. The Committee does not intend this subsection to diminish, supersede, or replace the responsibilities, authorities, or role of S&T's TechSolutions Program.

Sec. 202. Testing, Evaluation, and Standards.

This section establishes a Division of Test, Evaluation, and Standards, headed by a Director. The purpose of the Division is to assist S&T customers (Department components and others) in developing operational and performance testing plans and procedures, and developing and coordinating the adoption of national homeland security standards. Within the Division, the Deputy Director of Testing has responsibility to monitor and review operational testing and evaluation activities and the Standards Executive is responsible for supporting the development and adoption of voluntary standards.

The Committee strongly believes that when performance and operational testing is conducted by the same entity responsible for procurement, conflicts can arise. The difficulties experienced by the Department with the Advanced Spectroscopic Portal SBInet, and the Deepwater programs underscore the need for an independent entity to oversee technology testing. The Committee believes that this section is in line with the Secretary of Homeland Security's recent decision to pursue an independent testing and evaluation function for the Department.

Sec. 203. Peer Review.

This section requires the Under Secretary to develop and oversee guidelines for independent, external, scientific peer review of research projects. The Secretary must report on these activities not later than 60 days after completion of the first peer review.

The Committee believes that the integration of a peer review process into the Department's science and technology research and development efforts has the potential to enhance the effectiveness of these efforts. The Committee believes that peer review, a cornerstone of scientific advancement, should be conducted on homeland security research or technologies developed by S&T whenever possible.

Sec. 204. Office of Public-Private Partnerships.

Section 204 establishes the Office of Public-Private Partnerships, headed by a Director, with the responsibility to engage and initiate proactive outreach to persons in need of guidance on pursuing technology proposals with the Department, coordinate within the Department on technology announcements, promote interaction between the public and private sector to accelerate transition research, and conduct market analysis of technologies.

This section also creates the Rapid Review Division, a component of the Office of Public-Private Partnerships, which is responsible for establishing and publicizing an accessible, streamlined system to conduct timely reviews of unsolicited technology proposals (within 60 days of submission) and, upon completion of the review, submit promising proposals to the Director of Homeland Security Advanced Research Projects Agency (HSARPA) and other components for their consideration.

The Office may not consider or evaluate technology proposals submitted in response to a pending procurement.

Finally, this section authorizes the Director of the Office to establish up to three satellite offices and authorizes $30,000,000 for fiscal years 2011 and 2012 for the Office.

The Committee believes that the creation of a standing Office of Public-Private Partnership has great potential to enhance S&T's ability to meet the needs of its customers by fostering greater participation by firms that had not previously been able to access information and avenues to work with S&T. The Committee also strongly believes that the establishment of a Rapid Review Division will provide S&T with the ability to effectively assess unsolicited scientific proposals and, in short order, refer promising proposals that address customer-identified homeland security capability gaps to HSARPA or the appropriate component for further consideration.

TITLE III—Reports

Sec. 301. Directorate of Science and Technology Strategic Plan.

This section requires the Under Secretary to submit to Congress a strategic plan for the activities of S&T one year after enactment and every other year thereafter, to include long-term strategic goals; identification of programs that support these goals; connection of S&T programs to homeland security capability gaps identified by customers; role of the risk analysis in S&T programs; a technology transition strategy; and a description of policies on man-

agement, organization, and personnel. This plan must be prepared in accordance with applicable Federal requirements.

Sec. 302. Report on Technology Requirements.

Within 90 days of enactment and biannually thereafter, section 302 requires the Under Secretary to submit to Congress a list of detailed operational and technical requirements to Congress for projects having a Federal cost share of greater than $80,000,000. This section also requires that the Secretary submit a list of detailed operational and technical requirements for Department component projects with life-cycle costs of over $1,000,000,000.

Sec. 303. Report on Venture Capital Organization.

Not later than a year after enactment, this section requires the Secretary to report to Congress on the current role of the venture capital community in homeland security technology development, including its impact on small businesses, and recommendations about creating a non-profit venture capital organization for the purposes of delivering advanced homeland security technologies.

It specifically requires the Secretary to provide a description of how DHS works with emerging technology firms—in particular small business concerns, small businesses owned and operated by women, small businesses owned and operated by veterans, and minority-owned and operated businesses.

It also requires the Secretary to review venture capital organizations associated with the Department of Defense ("DoD"), like In-Q-Tel and OnPoint, to determine if these DOD models would work for DHS. The Secretary is required to deliver recommendations for how Congress could authorize the establishment of a venture capital organization for DHS and specifics on potential funding levels, activities for the organization (including the provision of technical assistance) and whether there should be set asides for minority-owned businesses and businesses located in economically disadvantaged areas.

The Committee believes that the establishment of a venture capital capability at DHS would not only foster greater homeland security innovation but would spur economic growth by creating new avenues for small businesses, including minority-owned and women-owned businesses, with promising technologies to receive critical financing.

The Committee is interested in reviewing the Secretary's recommendations on how a private, independent, not-for-profit organization designed to bridge the gap between homeland security needs and available technologies could be established to help develop advanced homeland security technologies.

In addition to information required in this section, the Committee would also find value in learning the extent to which the Secretary believes that such an organization should have experience in identifying and describing the technology requirements of the federal government; experience identifying the marketplace need for a product or service; knowledge of approaches to limit the inherent risk involved with research; experience with adapting commercially-oriented technologies for military use; and a history of working with leading venture capital institutions.

TITLE IV—Directorate of Science and Technology Programs

Sec. 401. Limitations on Research.

This section limits the Department from conducting research unless it addresses—to the greatest extent possible—a prioritized risk to the homeland (as identified by a Departmental risk analysis required in section 201 of this bill).

The Committee believes that, whenever possible, all S&T research, development, and acquisition decisions should be made under a risk-based framework. The Committee has found instances where S&T has made funding decisions without a robust analysis of the extent to which the potential technology would address a homeland security capability gap identified by S&T or a Department component. With this section, the Committee intends for S&T to focus research and development on areas that have been identified, through a proper risk analysis, as being a prioritized homeland security risk.

Sec. 402. University-Based Centers.

Section 402 authorizes $40,000,000 for the university-based centers program for fiscal year 2011 and $41,200,000 million for fiscal year 2012. This section specifies that existing areas of research, as defined in the Homeland Security Act, can include research of medical readiness and explosive countermeasures development.

Sec. 403. Review of University-Based Centers.

This section requires the Comptroller General (CG) to initiate, not later than 120 days after enactment of this Act, a study of the university-based centers for homeland security program and provide recommendations for improvements. Topics to be considered by the CG include: method of tasking university centers (and compare that to the method by which the Department tasks federally funded research and development centers and national labs); key areas for centers to consider; selection criteria for centers; optimal organization and role of centers; and measuring center successes. This section places a moratorium on the creation of new university-based centers until completion of this CG review to protect the existing programs that have been targeted for significant cuts in the fiscal year 2011 S&T budget request.

The Committee has a strong interest in seeing a greater utilization of the institutions that participate in the University-Based Centers program by S&T. Further, the Committee is concerned that S&T does not appear to appreciate that the Centers of Excellence program has the potential to be a valuable resource in its efforts to conduct homeland security research and development. The Committee has a strong interest in this study and intends, upon review of its findings, to work with S&T to put the program on a path to realizing its full potential.

Sec. 404. Cybersecurity Research and Development.

Section 404 requires the Under Secretary to support research, development, testing, evaluation, and transition of cybersecurity technology to prevent, protect against, detect, respond to, and recover from cyber attacks, with an emphasis on research relevant to large-scale, high-impact attacks. The section requires research in areas to include: secure protocols; intrusion detection technologies; cyber forensics and attack attribution; recovery methodologies; tools, testing, and modeling; control systems; and secure software. It requires the Under Secretary to coordinate with the Under Sec-

retary for National Protection and Programs Directorate and the heads of other relevant Federal departments and agencies.

This section authorizes the Secretary to establish a Cybersecurity Preparedness Consortium for purposes of providing training to State and local first responders for preparing for and responding to cyber attacks and coordination of cybersecurity preparedness training activities. Members of the consortium shall consist of academic, nonprofit, and government partners that have demonstrated expertise in cybersecurity training, a demonstrated ability to utilize existing DHS course and expertise, and a demonstrated ability to coordinate with the National Domestic Preparedness Consortium and other DHS training. At least three participating academic institutions are required to be qualified historically-Black colleges, Hispanic-serving institutions, Tribal colleges or universities, or some combination thereof.

This section authorizes the Secretary to establish a cybersecurity training center to provide training courses to State and local first responders to improve preparedness and response capabilities to cyber attacks.

It authorizes $75,000,000 for DHS cybersecurity activities in fiscal year 2011 and the same for fiscal year 2012.

Since 2007, the Committee has conducted eleven oversight hearings on various aspects of the cybersecurity threat. In the course of this oversight, the Committee has repeatedly received troubling testimony from experts inside and outside of the Federal government as to the extent to which bad actors in cyberspace have a distinct advantage over those attempting to secure their networks. Specifically, the Committee has received testimony as to the ease with which bad actors are able to mask the origination points for cyber intrusions and, even, attacks. Enhanced investment in cybersecurity research is critical to establishing effective attribution systems to track down the perpetrators of cyber intrusions.

Sec. 405. National Research Council Study of Cybersecurity Incentives.

Not later than 90 days after enactment, this section requires the Under Secretary and the Under Secretary for National Protection and Programs to seek to enter into agreement with National Academy of Sciences to conduct a study to assess methods that might be used to promote market mechanisms that further cybersecurity in the private sector. The assessment shall consider liability considerations, mandated reporting, regulation, certification, accounting, and cybersecurity risk insurance. Not later than two years after enactment, the Secretary is required to submit the results of the study, together with the Secretary's feedback and recommendations. To carry out the study, this section authorizes $500,000.

Sec. 406. Research on Cyber Compromise of Infrastructure.

Section 406 requires the Secretary, in collaboration with other national security and intelligence agencies, to conduct research to determine if the security of Federally-owned critical electric infrastructure has been compromised. The research should assess: the extent of compromise; identification of attackers; method of penetration; ramifications of compromise; and recommended mitigation activities. The Secretary is required to report to Congress on the

findings of the research, not later than 30 days after the completion of the project.

The Committee's Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology held four hearings on cybersecurity vulnerabilities, including cyber penetrations of government systems. The Committee believes that investigatory research required under this section, by fostering greater understanding within the Federal government about the extent to which systems have been compromised, will provide a basis for enhanced Federal mitigation, preparedness, response, and recovery from damaging cyber incursions and attacks.

Sec. 407. Dual-Use Terrorist Risks from Synthetic Genomics.

This section expresses the sense of Congress that synthetic genomics has potential to bring about great advances in biotechnology but, at the same time, there are homeland security risks since it also has the potential to be used as a weapon.

Section 407 requires the Under Secretary to report to Congress, not later than one year after enactment, as to the homeland security implications of the dual-use nature of synthetic genomics. If the Under Secretary determines that further research is appropriate, S&T may study the extent to which legitimate customers seeking synthetic genomics can be differentiated from potential terrorists or other malicious actors and develop enhanced security recommendations for screening software, protocols, and to address other capability gaps identified by the research.

Sec. 408. Underwater Tunnel Security Demonstration Project.

This section requires the Under Secretary, in consultation with the Assistant Secretary for TSA, to conduct a demonstration project for technologies to enhance the security of underwater public transportation tunnels. At least one of the technologies tested should be inflatable plugs. A report is required to Congress on the findings within 180 days of enactment.

Sec. 409. Threats Research and Development.

Section 409 authorizes the Under Secretary to conduct technology research, testing, evaluation, and transition activities to protect the Nation from biological, agricultural, and chemical threats. Such research could include detection, identification, counter measures, threat assessments, surveillance, forensics, and recovery activities. Additionally, the Under Secretary is authorized to produce risk assessments for biological, agricultural, and chemical threats, used to inform and guide the threat assessments and determinations made by the Secretary.

The Committee recognizes the important work done by the Department in producing risk assessments for chemical, biological, radiological, and nuclear threats. As the methodology used to develop the assessments evolves, the Committee believes that the Under Secretary should convene an interagency task force to assess and provide recommendations to the Under Secretary as to the adequacy of the methodology. The Under Secretary would not be bound by these recommendations, and they are not intended to be an approval or disapproval; rather, the task force will provide the Secretary with an objective view of the extent to which the proposed methodology will best meet the Department's needs in developing the risk assessments.

Sec. 410. Maritime Domain Awareness and Maritime Security Technology Test, Evaluation, and Transition Capabilities.

This section requires the Secretary to establish capabilities for conducting global maritime domain awareness and maritime security technology test, evaluation and transition. These efforts should focus on complementing existing efforts and avoiding duplication.

The Committee believes that the development of maritime testing, evaluation, and transition capabilities will enhance the Department's ability to deploy homeland security technology that can withstand the unique elements of the maritime environment.

Sec. 411. Rapid Biological Threat Detection and Identification.

Section 411 requires the Under Secretary assess whether DHS would benefit from technology to assist DHS personnel at ports of entry with entry and exit screening to rapidly detect infectious diseases among travelers. It requires the Under Secretary to initiate research and development of such technology, to the extent possible, if the Under Secretary determines that such research should be undertaken.

The Committee is concerned that the Department has not thoroughly considered the potential benefits and mechanisms of screening incoming travelers at the borders and ports of entry for communicable illnesses such as influenza. The Committee believes that accurate rapid diagnostic tools could help ensure timely triage and care of people not only at ports of entry, but also at points of care, leading ultimately to a more judicious use of limited medical countermeasures, including those in the Strategic National Stockpile.

The Committee is mindful of the unique mission areas for which different agencies are responsible, but also recognizes that homeland security is a cross-cutting venture, and the Department should have the ability and necessary cooperation to develop needed scientific and technological tools to fulfill its security responsibilities to the Nation. Should DHS assess that the potential benefits of such screening are a significant means of preventing infectious disease from threatening the homeland, the Department shall have the authority to do so, although the Committee believes that ideally, development and procurement of screening devices should be a joint venture between DHS and the Department of Health and Human Services (HHS).

Sec. 412. Educating the Public About Radiological Threats.

This section requires the Secretary to develop a public awareness campaign regarding radiological threats, including: a clear explanation of the dangers of radiological materials; explanation of radiation exposure levels; and actions that citizens can take regarding evacuation, decontamination, and treatment.

It also requires a plan for post-event recovery from a radiological incident or terrorist attack, including: definition of the dividing line between response and recovery; consideration of multiple attack scenarios and multiple recovery strategies; and consideration of economic, health, and psychological effects.

The Committee strongly believes that a well-informed and well-prepared public is a vital component to defend against a terrorist attack. Empowering the public with information on what to do in the event of a radiological or nuclear attack has the potential of

dramatically decreasing the rate of death and injury. The Committee, therefore, directs the Secretary to work with State, local, and tribal authorities to develop materials to communicate to the public the risks faced and actions necessary to be taken in the event of such an attack.

Sec. 413. Rural Resilience Initiative.

Section 413 requires the Secretary to conduct research to aid State, local, and tribal leaders to help anticipate and forestall terrorist events in rural communities. These activities should include: outreach activities with rural communities; examination of community use of resilience capabilities and assets; establishment of a community resilience baseline template; plans to address community resilience needs; education for community leaders and first responders on resilience; and creation of a mechanism for such research to serve communities across the nation.

The Committee notes the relative void in research that addresses rural communities and encourages the Department to conduct research and implementation through outreach activities with rural communities. The outcomes of this activity can serve as a model for national adoption. By assisting rural communities in disaster preparedness and resiliency, these communities will return to productivity much faster following an event, resulting in more stable environments in which to live and work, enhancing the quality of life in rural America and creating economic advantages for these resilient communities.

The Committee recognizes the important functions of the Southeast Regional Research Initiative (SERRI) program. Through this initiative, a diverse group of research universities along with Federal partners work with state and local governments to identify and research homeland security challenges within the region, particularly those with national implications. The Committee encourages the rural resiliency work of the Department to continue through this and other programs.

Sec. 414. Sense of Congress Regarding the Need for Interoperability Standards for Internet Protocol Video Surveillance Technology.

This section expresses the sense of Congress that the development of interoperability standards are necessary to realize the full security benefits of Internet Protocol (IP) video surveillance, an emerging homeland security technology and encourages S&T to work with the private sector and other Federal stakeholders to develop such standards.

Sec. 415. Homeland Security Science and Technology Fellows Program.

Section 415 requires the Secretary, acting through the Under Secretary, to establish the Homeland Security Science and Technology Fellows Program for scientists to be placed in relevant scientific and technological positions within S&T and components of the Department in paid positions for up to two years. Program participants must be currently enrolled in or be graduates of postgraduate scientific or engineering programs. The Under Secretary is directed to coordinate with the Chief Security Officer to facilitate and expedite the provision of security clearances to fellows, as appropriate.

The Committee is concerned that American students are falling behind in the essential subjects of math and science, putting our position in the global economy at risk. As a result, there has been a steady decline in levels of expertise in science and technology throughout the Nation, which, has a detrimental impact on homeland security capabilities. The Committee intends for this program to support placement, development, and advancement of American scientists and engineers within the field of homeland security.

Sec. 416. Biological Threat Agent Assay Equivalency.

This section authorizes the Under Secretary, in consultation with the Director for the Centers for Disease Control, to develop assay equivalency standards to facilitate the establishment of consistent biological threat identification by Federally-operated bio-monitoring programs. Upon the development of the assay equivalency standards, it requires the Secretary to apply the biological assay equivalency standards to DHS' bio-monitoring programs and make the standards available to other Federal agencies.

The Committee recognizes that there are many Federal, State, local, and private sector actors that contribute to the biological threat identification mission through a variety of programs. The Committee intends for this section to ensure that the different types of assays available should meet a common standard so that the results of any assay will be considered reliable throughout the homeland security community.

Sec. 417. Study of Feasibility and Benefit of Expanding or Establishing Program to Create a New Cybersecurity Capacity Building Track at Certain Institutions of Higher Education.

Section 417 requires the Secretary, in coordination with the National Science Foundation, to commission a study by a non-profit research institution to assess how best to create a new cybersecurity or information assurance capacity building track at colleges and universities that are not designated as National Centers of Academic Excellence in Information Assurance Education or National Centers of Academic Excellence in Research. The study should consider the feasibility and potential benefit of allowing community colleges and other institutions offering certificates or industry-recognized credentials to participate in the Federal Cyber Service Scholarship for Service Program or creating a parallel program within the Department. The Secretary is required to transmit the study to Congress not later than 30 days after receiving it.

Since 2007, the Committee's eleven oversight hearings on cybersecurity vulnerabilities in the public and private sectors underscore the need for more focus on information assurance in the computer science and information technology fields. This study is intended to help identify an official educational mechanism or certification to promote the importance of information assurance.

Sec. 418. Sense of Congress Regarding Centers of Excellence.

This section expresses the sense of Congress that the Centers of Excellence program has the potential to be a very useful tool in developing defensive countermeasures to enhance the security of critical infrastructure, prevent terrorism, and enhance S&T's efforts to research and develop homeland security technologies.

Sec. 419. Assessment, Research, Testing, and Evaluation of Technologies to Mitigate the Threat of Small Vessel Attack.

This section authorizes the Under Secretary to assess what technologies are available to mitigate the threat of small vessel attacks in secure zones of ports and conduct research, testing, and evaluation of such technologies.

Many of the elements of the Department, including the Coast Guard, U.S. Customs and Border Protection, and the Domestic Nuclear Detection Office have identified small maritime craft as a credible threat vector. The Committee supports research into technologies focused on this unique homeland security challenge.

Sec. 420. Research and Development Projects.

Section 420 extends through 2012 the authority of the Secretary to make expenditures to carry out basic, applied, and advanced research and development projects through non-standard acquisitions procedures, commonly referred to as "other transaction authority", instead of the Federal Acquisitions Regulation (FAR). Additionally, it requires that each time the Under Secretary intends to use other transaction authority, the Under Secretary submit a specific proposal to the Secretary that sets for the rationale for why the FAR process is not feasible or appropriate in that particular case. The Secretary, in turn, is responsible for evaluating this proposal and may only delegate this responsibility to the Under Secretary for Management.

This section requires an annual report to Congress as to the exercise of other transaction authority that includes the subject areas that were researched, the extent of the cost-share, and the extent to which the use of this authority has addressed a homeland security gap.

The Secretary is required to develop training for acquisitions staff who are involved in the exercise of other transaction authority.

The exercise of other transaction authority is subject to review by the Comptroller General on an ongoing basis.

The Committee notes that S&T has repeatedly argued that the utilization of other transaction authority provides greater flexibility to attract and work with nontraditional contractors—most especially small businesses—to research, develop, and test innovative technologies. However, the Committee received testimony at a hearing entitled "Other Transaction Authority: Flexibility at the Expense of Accountability?" on February 7, 2008 that the exercise of this authority carries the risk of reduced accountability and transparency-in part because they are exempt from certain federal acquisition regulations and cost accounting standards. At that hearing, the Government Accountability Office testified that though the Department has internal processes that govern the utilization of this authority, "further development of the department's policies and strengthening of its workforce are needed to promote successful use of the authority."

The Committee believes that the transparency and accountability enhancements in this section will bring S&T in line with the Department of Defense and other Federal agencies that have similar contracting authority.

Sec. 421. National Urban Security Technology Laboratory.

This section authorizes the National Urban Security Technology Laboratory—formerly the "Environmental Measurements Laboratory"—for Fiscal Years 2011 and 2012. Requires the Under Secretary to utilize the laboratory to test, evaluate, and analyze homeland security technologies in the field and in the laboratory.

The transformation of the laboratory since it was transferred to the Department under the Homeland Security Act of 2002 has added a unique capability for the Department as it has truly become a Homeland Security Laboratory. The Committee believes that the new focus at the laboratory on practical test and evaluation for first responder equipment and tactics, as well as other capabilities to support the overall test and evaluation mission as required in section 202, make the National Urban Security Technology Laboratory a critical asset to the Department's mission.

TITLE V—Domestic Nuclear Detection Office

Sec. 501. Authorization of Appropriations.

This section authorizes $305,840,000 for Fiscal Year 2011 and $315,005,000 for Fiscal Year 2012 for the Domestic Nuclear Detection Office (DNDO).

Sec. 502. Domestic Nuclear Detection Office Oversight.

This section expresses the sense of Congress that S&T should conduct basic and innovative research and non-developmental testing for DNDO. Not later than 90 days after enactment, it requires the Director of DNDO to begin an internal review of DNDO project selection methodology, research, development, testing, and evaluation (RDT&E) methodologies and priorities in order to set policy and track progress of RDT&E projects. In carrying out the review, the Director shall identify processes for research funding, describe roles, responsibilities, and procedures for RDT&E, implement a research tracking system, implement a system to provide updates to customers, evaluate whether first responder needs are being addressed, establish a method to collect feedback, identify appropriate investment levels, and establish a formal merit review process.

Not later than a year after the completion of review, the Director shall submit a report to the Secretary and Congress containing the findings of the review. This section requires the Inspector General, 120 days after enactment and annually thereafter, to update Congress on the status of implementation of this section.

The Committee notes that this section is intended to create requirements for DNDO that are parallel to those for S&T under sections 201 and 202 of this Act. The Committee supports the Secretary's recent decision to pursue an independent testing and evaluation function for the Department, as well as to require the Science and Technology directorate to conduct basic and innovative research for nuclear and radiological detection.

Sec. 503. Strategic Plan and Funding Allocations for Global Architecture.

This section requires the Secretary to submit, within 180 days of enactment, a strategic plan for the domestic component of the global nuclear detection architecture to deter and detect the transport of nuclear materials by all means possible. The plan shall address technological and non-technological methods to increase detection; the deterrent impact of a global detection architecture on would-be

terrorists; necessary enhancements to existing technologies; and risk-based analysis of asset deployment. The plan shall be conducted in consultation with the Secretaries of Energy, State, Defense, Justice, the Nuclear Regulatory Commission, and the Intelligence Community.

The Committee believes that a coherent Global Nuclear Detection Architecture is essential in protecting the country from radiological or nuclear terrorism and is consistent with a layered, defense-in-depth strategy. To achieve this goal, the Committee believes that maximum coordination with the other relevant agencies is critical.

Sec. 504. Radiation Portal Monitor Alternatives.

Section 504 expresses the sense of Congress that in light of the Secretary's decision not to certify Advanced Spectroscopic Portal Monitors for primary screening, viable alternatives should be investigated. It requires the Director of DNDO to report within 90 days about alternatives to existing technologies that would provide the Department with a significant increase in operational effectiveness for primary screening for radioactive materials.

The Committee supports the Secretary's determination that the development and procurement of the Advanced Spectroscopic Portal should be pursued for secondary inspection, rather than primary inspection. In light of this determination, however, the Committee strongly believes that research and development efforts to improve primary inspection efficacy and performance must be enhanced.

Sec. 505. Authorization of Securing the Cities Initiative.

Section 505 sets forth Congressional findings that the Securing the Cities (STC) Initiative uses next generation radiation detection technology, leverages the technologies used as U.S. ports of entry, has fostered cooperation between Federal, State, and local partners, and represents a critical national radiation detection capability. This section authorizes the program for fiscal year 2011 at $20,000,000 and fiscal year 2012 at $10,000,000, and at least two additional cities that participate in the Urban Area Security Initiative are also authorized to participate in STC.

This provision reflects the language in H.R. 2611, which authorized the Securing the Cities Initiative and was passed by the House on January 20, 2010.

The Committee has supported the Securing the Cities Initiative in a bipartisan manner since its inception. The Committee's favorable adoption of H.R. 4842 on April 15, 2010 is only the most recent in a series of favorable votes to promote Federal support of this program. On January 12, 2010, the Committee voted favorably to report out H.R. 2611, which would permanently authorize the program; subsequently, the House passed the bill by voice vote. Strong, bipartisan support for Securing the Cities also was shown in the 110th Congress for H.R. 5531, which would have authorized the Initiative, and which both the Committee and the House voted to support. The House has also voiced its approval through the appropriations process: a bipartisan amendment to appropriate $40 million passed on June 24, 2009 for the Initiative's continuation in fiscal year 2010.

Given that a radiological attack in a major urban area could easily have significant ripple effects throughout the Nation, the Com-

mittee believes the Securing the Cities Initiative should be treated as a national capability with sustained Federal funding. The Committee supports Securing the Cities because this vital program has fostered unprecedented collaboration and coordination among its many Federal, State, and local partners. The Committee believes that the program's record of success will enhance the security of urban areas against radiological and other types of threats. Law enforcement agencies in New York, New Jersey, and Connecticut have all benefited from this collaboration, and the Committee commends the Domestic Nuclear Detection Office, Department of Homeland Security, for its development and oversight of this unified strategy. The Securing the Cities Initiative is the only DHS program dedicated specifically to reducing the risk of radiological and nuclear terrorism through targeted detection.

The detonation of an improvised nuclear device or a radiological dispersal device in a metropolitan area of the United States would have devastating consequences due to loss of life, destruction of property, and economic repercussions. President Obama emphasized this concern, especially for major urban areas like New York and London, at the National Security Summit in April 2010. He also pledged to bring to justice those responsible for the attempted car bombing on Times Square on May 1, 2010, an event that underscored how New York City remains the top terrorist target. The Securing the Cities Initiative is the only program dedicated specifically to reducing the risk of radiological and nuclear terrorism through targeted detection. Enactment of H.R. 4842 into law will ensure that this capability is permanently authorized, and that the benefits of the program are perpetuated not only in the New York metropolitan area, but across the Nation.

TITLE VI—Clarifying Amendments

Sec. 601. Federally Funded Research and Development Centers.

This section encourages the homeland security federally funded research and development center to consider research proposals made by the Chairman and Ranking Member of an appropriate congressional committee in a bipartisan fashion.

It encourages a federally funded research and development center to provide a copy of any report it produces to an appropriate congressional committees, upon request.

It also requires the Secretary to review and revise, as appropriate, the personnel conflict of interest policies pertaining to federally funded research and development centers.

Sec. 602. Elimination of Homeland Security Institute.

Section 602 repeals the Homeland Security Institute from the Homeland Security Act. The Committee notes that the Department uses its authority under Section 305 of the Homeland Security Act of 2002 to create federally funded research and development centers, rendering this provision moot.

This provision is a technical correction to the Homeland Security Act. The Committee does not intend for this section to have any impact on the Departmental Federally Funded Research and Development Centers.

Sec. 603. GAO Study of DOE National Laboratories.

This section requires the Comptroller General to conduct a study to assess the relationship between DHS and the Department of Energy National Laboratories, and submit recommendations for improving the relationship.

The Committee recognizes the enormous benefit that the Department receives from its strong partnership with the Department of Energy National Laboratories and encourages S&T to explore new opportunities for collaboration and the leveraging of National Laboratory expertise to address homeland security capability gaps.

TITLE VII—Commission on the Protection of Critical Electric and Electronic Infrastructures

Sec. 701. Commission on the Protection of Critical Electric and Electronic Infrastructures.

Section 701 establishes the Commission on the Protection of Critical Electric and Electronic Infrastructures, whose purpose is to assess vulnerabilities of this infrastructure and provide a clear and comprehensive strategy and specific recommendations for securing this infrastructure. The Commission is required to give particular attention to threats that can cause widespread disruption or damage to this infrastructure including cyber attacks and physical attacks.

This section sets forth the composition, powers, and responsibilities of the Commission, and provides $4,000,000 for fiscal years 2011 and 2012 from sums authorized in section 101.

The Committee intends for this new Commission to take up where the former Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack—often referred to as the EMP Commission—left off when its authorization expired in December of 2008. The new Commission is envisioned to go beyond the scope of the original Commission to address all electromagnetic threats to all U.S. Critical Infrastructure Sectors.

The Committee believes that the EMP Commission, established pursuant to Public Law 106–398, has done the Nation an invaluable service by highlighting a potential vulnerability to critical electric and electronic infrastructure—an attack or other incident involving electromagnetic phenomena. The Committee has a longstanding interest in enhancing security for the electric grid. In fact, on October 18, 2005, the Subcommittees on Emerging Threats, Cybersecurity, Science and Technology and Emergency Preparedness, Science, and Technology held a joint hearing entitled "SCADA and the Terrorist Threat: Protecting the Nation's Critical Control Systems." The Committee took another look at our cybersecurity posture with respect to the electric and electronic grid on October 17, 2007, when the Subcommittee on Emerging Threats, Cybersecurity, Science and Technology held a hearing entitled "The Cyber Threat to Control Systems: Stronger Regulations are Necessary to Secure Electric Grid." More recently, on July 21, 2009, the Subcommittee on Emerging Threats, Cybersecurity, Science and Technology held a hearing entitled "Securing the Modern Electric Grid from Physical and Cyber Attacks."

From our extensive oversight work, the Committee has come to recognize that there is an ongoing need for study of this homeland security vulnerability and for operators of critical infrastructure to have greater awareness and guidance on the development of miti-

gation strategies. By authorizing a new Commission on the Protection of Critical Electric and Electronic Infrastructure, the Committee intends for this critical study to continue and mitigation strategies to be developed.

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)* * *

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

* * * * * * *

TITLE II—INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION

* * * * * * *

Subtitle C—Information Security

* * * * * * *

Sec. 226. Cybersecurity Preparedness Consortium.
Sec. 227. Cybersecurity Training Center.

Subtitle D—[Office of] Science and Technology

Sec. 231. Establishment of [office] *Office of Science and Technology*; director.

* * * * * * *

Sec. 238. Research prioritization and requirements.
Sec. 239. Professional development.
Sec. 240. Tracking systems, research milestones, and customer feedback.

TITLE III—SCIENCE AND TECHNOLOGY IN SUPPORT OF HOMELAND SECURITY

* * * * * * *

[Sec. 312. Homeland Security Institute.
[Sec. 313. Technology clearinghouse to encourage and support innovative solutions to enhance homeland security.]
Sec. 313. Office of Public-Private Partnerships.

* * * * * * *

Sec. 318. Strategic plan.
Sec. 319. Homeland Security Science and Technology Fellows Program.
Sec. 320. Biological threat agent assay equivalency program.

* * * * * * *

TITLE II—INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION

* * * * * * *

Subtitle C—Information Security

* * * * * * *

SEC. 226. CYBERSECURITY PREPAREDNESS CONSORTIUM.

(a) IN GENERAL.—To assist the Secretary in carrying out the requirements of section 404(a) of the Homeland Security Science and Technology Authorization Act of 2010, the Secretary may establish a consortium to be known as the "Cybersecurity Preparedness Consortium".

(b) FUNCTIONS.—The Consortium shall—

(1) provide training to State and local first responders and officials specifically for preparing and responding to cybersecurity attacks;

(2) develop and update a curriculum and training model for State and local first responders and officials;

(3) provide technical assistance services to build and sustain capabilities in support of cybersecurity preparedness and response;

(4) conduct cybersecurity training and simulation exercises to defend from and respond to cyber attacks; and

(5) coordinate all cybersecurity preparedness training activities conducted by the Department.

(c) MEMBERS.—The Consortium shall consist of academic, nonprofit, and government partners that—

(1) have demonstrated expertise in developing and delivering cybersecurity training in support of homeland security;

(2) have demonstrated ability to utilize existing courses and expertise developed by the Department;

(3) have demonstrated ability to coordinate with the National Domestic Preparedness Consortium and other training programs within the Department; and

(4) include at least 3 academic institutions that are any combination of historically Black colleges and universities, Hispanic-serving institutions, or Tribal Colleges and Universities, that fulfill the criteria of paragraphs (1), (2) and (3) of this subsection.

(d) DEFINITIONS.—In this section:

(1) HISTORICALLY BLACK COLLEGE OR UNIVERSITY.—The term "historically Black college or university" has the meaning given the term "part B institution" in section 322(2) of the Higher Education Act of 1965 (20 U.S.C. 1061(2)).

(2) HISPANIC-SERVING INSTITUTION.—The term "Hispanic-serving institution" has the meaning given that term in section 502 of the Higher Education Act of 1965 (20 U.S.C. 1101(a)).

(3) TRIBAL COLLEGE OR UNIVERSITY.—The term "Tribal College or University" has the meaning given that term in section 316(b) of the Higher Education Act of 1965 (20 U.S.C. 1059c(b)).

SEC. 227. CYBERSECURITY TRAINING CENTER.

The Secretary may establish where appropriate a Cybersecurity Training Center to provide training courses and other resources for State and local first responders and officials to improve preparedness and response capabilities.

Subtitle D—[Office of] Science and Technology

SEC. 231. ESTABLISHMENT OF OFFICE *OF SCIENCE AND TECHNOLOGY*; DIRECTOR.

(a)* * *

* * * * * * *

SEC. 238. RESEARCH PRIORITIZATION AND REQUIREMENTS.

(a) REQUIREMENT.—The Secretary shall—

(1) by not later than 180 days after the date of enactment of this section, establish requirements for how basic and applied homeland security research shall be identified, prioritized, funded, tasked, and evaluated by the Directorate of Science and Technology, including the roles and responsibilities of the Under Secretary for Science and Technology, the Under Secretary for Policy, the Under Secretary for Management, the Director of the Office of Risk Management and Analysis, and the heads of operational components of the Department; and

(2) to the greatest extent possible, seek to publicize the requirements for the purpose of informing the Federal, State, and local governments, first responders, and the private sector.

(b) CONTENTS.—In the requirements, the Secretary shall—

(1) identify the Directorate of Science and Technology's customers within and outside of the Department;

(2) describe the risk formula and risk assessment tools that the Department considers to identify, prioritize, and fund homeland security research projects;

(3) describe the considerations to be used by the Directorate to task projects to research entities, including the national laboratories, federally funded research and development centers, and university-based centers;

(4) describe the protocols to be used to assess off-the-shelf technology to determine if an identified homeland security capability gap can be addressed through the acquisition process instead of commencing research and development of technology to address that capability gap;

(5) describe the processes to be used by the Directorate to strengthen first responder participation in identifying and prioritizing homeland security technological gaps by—

(A) soliciting feedback from appropriate national associations and advisory groups representing the first responder community and first responders within the components of the Department;

(B) establishing and promoting a publicly accessible portal to allow the first responder community to help the Directorate develop homeland security research and development goals; and

(C) establishing a mechanism to publicize the Department's funded and unfunded homeland security technology priorities; and

(6) include such other requirements, policies, and practices as the Secretary considers necessary.

(c) ACTIVITIES IN SUPPORT OF THE RESEARCH PRIORITIZATION AND REQUIREMENTS.—Not later than one year after the date of the issuance of the requirements, the Secretary shall—

(1) establish, through the Under Secretary for Science and Technology and Under Secretary for Management, a mandatory workforce program for the Directorate's customers in the Department to better identify and prioritize homeland security capability gaps that may be addressed by a technological solution based on the assessment required under section 239(a)(2);

(2) establish a system to collect feedback from customers of the Directorate on the performance of the Directorate, that includes metrics for measuring customer satisfaction and the usefulness of any technology or service provided by the Directorate; and

(3) any other activities that the Secretary considers to be necessary to implement the requirements.

(d) QUARTERLY UPDATES ON IMPLEMENTATION.—One hundred and twenty days after the date of enactment of this section, and on a quarterly basis thereafter, the Inspector General of the Department shall submit a quarterly update to the appropriate congressional committees on the status of implementation of the research prioritization and requirements and activities in support of such requirements.

(e) RISK ANALYSIS.—In carrying out subsection (b)(2), the Secretary shall—

(1) submit to the appropriate congressional committees by not later than one year after the date of enactment of this subsection and annually thereafter—

(A) a national-level risk assessment, describing and prioritizing the greatest risks to the homeland, that includes vulnerability studies, asset values (including asset values for intangible assets), estimated rates of occurrence, countermeasures employed, loss expectancy, cost/benefit analyses, and other practices generally associated with producing a comprehensive risk analysis;

(B) an analysis of the Directorate's approach to mitigating the homeland security risks identified under subparagraph (A) through basic and applied research, development, demonstration, testing, and evaluation activities;

(C) an analysis, based on statistics and metrics, of the effectiveness of the Directorate in reducing the homeland security risks identified under subparagraph (A) through the deployment of homeland security technologies researched or developed by the Directorate;

(D) recommendations for how the Directorate should modify or amend its research and development activities in order to reduce the risks to the homeland identified under subparagraph (A);

(E) a description of how the analysis required under subparagraph (A) shall be used to inform, guide, and prioritize the Department's homeland security research and development activities; and

(F) a description of input from other relevant Federal, State, or local agencies and relevant private sector entities

in conducting the risk analysis required by subparagraph (A); and

(2) conduct research and development on ways to most effectively communicate information regarding the risks identified under paragraph (1) to the media as well as directly to the public, both on an ongoing basis and during a terrorist attack or other incident.

(f) REPORT ON HSARPA ACTIVITIES.—

(1) IN GENERAL.—Consistent with the Federal Acquisition Regulation and any other relevant Federal requirements, not later than 60 days after the date of enactment of this subsection and annually thereafter, the Secretary shall submit a report to the appropriate congressional committees containing the research, development, testing, evaluation, prototyping, and deployment activities undertaken by the Homeland Security Advanced Research Projects Agency during the previous fiscal year, including funds expended for such activities in the previous fiscal year.

(2) CONTENTS.—For each activity undertaken, the report shall—

(A) describe the corresponding risk analysis performed by the Department that supports the decision to undertake that activity; and

(B) describe the efforts made to transition that activity into a Federal, State, or local acquisition program.

(3) ADDITIONAL ACTIVITIES.—The Secretary shall include in each report a description of each proposal that was reviewed in the period covered by the report by the Director of the Homeland Security Advanced Research Projects Agency under section 313(d)(3), including a statement of whether the proposal received a grant, cooperative agreement, or contract from the Director.

SEC. 239. PROFESSIONAL DEVELOPMENT.

(a) REPORTING REQUIREMENT.—Sixty days before establishing the mandatory workforce program as required by section 238(c)(1), the Secretary shall report to the appropriate congressional committees on the following:

(1) A description of how homeland security technological requirements are developed by the Directorate of Science and Technology's customers within the Department.

(2) An assessment of whether Department employees receive adequate and appropriate job training to allow them to identify, express, and prioritize homeland security capability gaps.

(3) A plan for how the Directorate, in coordination with the Domestic Nuclear Detection Office and other Department components, can enhance and improve technology requirements development and the technology acquisition process, to accelerate the delivery of effective, suitable technologies that meet performance requirements and appropriately address an identified homeland security capability gap.

(4) An assessment of whether Congress should authorize, in addition to the program required under section 238(c)(1), a training program for Department employees to be trained in requirements writing and acquisition, that—

(A) is prepared in consultation with the Department of Veterans Affairs Acquisition Academy and the Defense Acquisition University; and

(B) if the Secretary determines that such additional training should be authorized by Congress, includes specification about—

(i) the type, skill set, and job series of Department employees who would benefit from such training, including an estimate of the number of such employees;

(ii) a suggested curriculum for the training;

(iii) the type and skill set of educators who could most effectively teach those skills;

(iv) the length and duration of the training;

(v) the advantages and disadvantages of training employees in a live classroom, or virtual classroom, or both;

(vi) cost estimates for the training; and

(vii) the role of the Directorate in supporting the training.

(b) USE OF RESEARCH AND DEVELOPMENT CENTER.—The Secretary is encouraged to use a federally funded research and development center to assist the Secretary in carrying out the requirements of this section.

SEC. 240. TRACKING SYSTEMS, RESEARCH MILESTONES, AND CUSTOMER FEEDBACK.

(a) IN GENERAL.—In establishing a system to collect feedback under section 238(c)(2), the Secretary shall—

(1) establish a system to monitor and account for homeland security research milestones;

(2) create a formal process for collecting feedback from customers on the effectiveness of the technology or services delivered by Directorate of Science and Technology, including through randomized sampling, focus groups, and other methods as appropriate; and

(3) establish standards and performance measures to be met by the Directorate in order to provide high-quality customer service.

(b) SYSTEM.—The system established under subsection (a)(1) shall identify and account for research milestones to monitor the progress of Directorate of Science and Technology research, development, testing, and evaluation activities, and collect information from the Directorate's customers about their level of satisfaction with the performance of the Directorate, including by—

(1) allowing the Directorate to provide regular reports to its customers regarding the status and progress of research efforts of the Directorate;

(2) collecting and evaluating customer feedback;

(3) allowing the Secretary to evaluate how a technology or service produced as a result of the Directorate's programs has affected homeland security capability gaps; and

(4) allowing the Secretary to report the number of products and services developed by the Directorate that have been transitioned into acquisition programs.

(c) GUIDANCE.—The Under Secretary for Science and Technology shall publicize and implement guidance for homeland security re-

searchers funded by the Directorate on setting valid initial and subsequent research milestones.

(d) REPORT.—The Under Secretary shall submit a report to the appropriate congressional committees—

(1) by not later than one year after the date of enactment of this section identifying what actions have been taken to carry out the requirements of this section; and

(2) annually thereafter describing—

(A) research milestones for each large project with a Federal cost share greater than $80,000,000 that has been successfully met and missed, including for each missed milestone, an explanation of why the milestone was missed; and

(B) customer feedback collected and the success of the Directorate in meeting the customer service performance measures and standards, including an evaluation of the effectiveness of the technology or services delivered by the Directorate.

TITLE III—SCIENCE AND TECHNOLOGY IN SUPPORT OF HOMELAND SECURITY

* * * * * * *

SEC. 302. RESPONSIBILITIES AND AUTHORITIES OF THE UNDER SECRETARY FOR SCIENCE AND TECHNOLOGY.

(a) IN GENERAL.—The Secretary, acting through the Under Secretary for Science and Technology, shall have the responsibility for—

(1)* * *

* * * * * * *

(4) conducting basic and applied research, development, demonstration, testing, and evaluation activities that are relevant to any or all elements of the Department, through both intramural and extramural programs, *that, to the greatest extent possible, addresses a prioritized risk to the homeland as identified by a risk analysis under section 226(e) of this Act* except that such responsibility does not extend to human health-related research and development activities;

* * * * * * *

(13) coordinating with other appropriate executive agencies in developing and carrying out the science and technology agenda of the Department to reduce duplication and identify unmet needs; **[**and**]**

(14) developing and overseeing the administration of guidelines for merit review of research and development projects throughout the Department, and for the dissemination of research conducted or sponsored by the Department**[**.**]***; and*

(15) developing and overseeing the administration of guidelines for peer review of research and development projects, including by—

(A) consulting with experts, including scientists and practitioners, about the research and development conducted by the Directorate of Science and Technology; and

(B) performing ongoing independent, external, scientific peer review—

(i) initially at the division level; or

(ii) when divisions conduct multiple programs focused on significantly different subjects, at the program level.

(b) REPORT ON TECHNOLOGY REQUIREMENTS.—

(1) IN GENERAL.—Within 90 days after the date of enactment of this subsection, and biannually thereafter, the Under Secretary shall, for each project having a Federal cost share greater than $80,000,000 that is conducted or funded by the Directorate of Science and Technology, provide to the appropriate congressional committees a list of detailed operational and technical requirements that are associated with the project.

(2) LARGE PROJECTS.—Within 90 days after the date of enactment of this subsection, and biannually thereafter, the Secretary shall, for each project conducted or funded by a component of the Department, other than the Directorate of Science and Technology, having a life-cycle cost greater than $1,000,000,000, provide to the appropriate congressional committees detailed operational and technical requirements that are associated with the project.

* * * * * * *

SEC. 305. FEDERALLY FUNDED RESEARCH AND DEVELOPMENT CENTERS.

(a) ESTABLISHMENT.—The Secretary, acting through the Under Secretary for Science and Technology, shall have the authority to establish or contract with 1 or more federally funded research and development centers to provide independent analysis of homeland security issues, or to carry out other responsibilities under this Act, including coordinating and integrating both the extramural and intramural programs described in section 308.

(b) CONGRESSIONAL TASKING.—Upon a request of the chairman and the ranking minority member of an appropriate congressional committee, a federally funded research and development center established under this section may perform independent analysis of homeland security issues and report its findings to the appropriate congressional committees and the Secretary.

(c) CONGRESSIONAL OVERSIGHT.—Federally funded research and development centers established under this section are encouraged, upon request of the chairman and the ranking minority member of an appropriate congressional committee, to provide to the committee a copy of any report it produces for the Department or any of its components.

(d) CONFLICTS OF INTEREST.—The Secretary shall review and revise, as appropriate, the policies of the Department relating to personnel conflicts of interest to ensure that such policies specifically address employees of federally funded research and development centers established under this section who are in a position to make or materially influence research findings or agency decisionmaking.

(e) ANNUAL REPORTS.—Each federally funded research and development center established under this section shall transmit to the

Secretary and appropriate congressional committees an annual report on the activities of the center.

* * * * * * *

SEC. 308. CONDUCT OF RESEARCH, DEVELOPMENT, DEMONSTRATION, TESTING AND EVALUATION.

(a)* * *

(b) EXTRAMURAL PROGRAMS.—

(1)* * *

(2) UNIVERSITY-BASED CENTERS FOR HOMELAND SECURITY.—

(A)* * *

(B) CRITERIA FOR DESIGNATION.—Criteria for the designation of colleges or universities as a center for homeland security, shall include, but are not limited to, demonstrated expertise in—

(i)* * *

* * * * * * *

(iii) Emergency and diagnostic medical services*, including medical readiness training and research, and community resiliency for public health and healthcare critical infrastructure*.

(iv) Chemical, biological, radiological, [and nuclear] *nuclear, and explosive* countermeasures or detection.

* * * * * * *

(d) TEST, EVALUATION, AND STANDARDS DIVISION.—

(1) ESTABLISHMENT.—There is established in the Directorate of Science and Technology a Test, Evaluation, and Standards Division.

(2) DIRECTOR.—The Test, Evaluation, and Standards Division shall be headed by a Director of Test, Evaluation, and Standards, who shall be appointed by the Secretary and report to the Under Secretary for Science and Technology.

(3) RESPONSIBILITIES, AUTHORITIES, AND FUNCTIONS.—The Director of Test, Evaluation, and Standards—

(A) is the principal adviser to the Secretary, the Under Secretary of Management, and the Under Secretary for Science and Technology on all test and evaluation or standards activities in the Department; and

(B) shall—

(i) prescribe test and evaluation policies for the Department, which shall include policies to ensure that operational testing is done at facilities that already have relevant and appropriate safety and material certifications to the extent such facilities are available;

(ii) oversee and ensure that adequate test and evaluation activities are planned and conducted by or on behalf of components of the Department in major acquisition programs of the Department, as designated by the Secretary, based on risk, acquisition level, novelty, complexity, and size of the acquisition program, or as otherwise established in statute;

(iii) review major acquisition program test reports and test data to assess the adequacy of test and evalua-

tion activities conducted by or on behalf of components of the Department; and

(iv) review available test and evaluation infrastructure to determine whether the Department has adequate resources to carry out its testing and evaluation responsibilities, as established under this title.

(4) DEPUTY DIRECTOR OF OPERATIONAL TEST AND EVALUATION.—Within the Division there shall be a Deputy Director of Operational Test and Evaluation, who—

(A) is the principal operational test and evaluation official for the Department; and

(B) shall—

(i) monitor and review the operational testing and evaluation activities conducted by or on behalf of components of the Department in major acquisition programs of the Department, as designated by the Secretary, based on risk, acquisition level, novelty, complexity, and size of the acquisition program, or as otherwise established in statute;

(ii) provide the Department with independent and objective assessments of the adequacy of testing and evaluation activities conducted in support of major acquisitions programs; and

(iii) have prompt and full access to test and evaluation documents, data, and test results of the Department that the Deputy Director considers necessary to review in order to carry out the duties of the Deputy Director under this section.

(5) STANDARDS EXECUTIVE.—Within this Division, there shall be a Standards Executive as described in Office of Management and Budget Circular A–119. The Standards Executive shall—

(A) implement the Department's standards policy as described in section 102(g); and

(B) support the development and adoption of voluntary standards in accordance with section 12(d) of the National Technology Transfer and Advancement Act of 1995 (15 U.S.C. 272 note).

(6) LIMITATION.—The Division is not required to carry out operational testing.

(7) EVALUATION OF DEPARTMENT OF DEFENSE TECHNOLOGIES.—The Director of Test, Evaluation, and Standards may evaluate technologies currently in use or being developed by the Department of Defense to assess whether they can be leveraged to address homeland security capability gaps.

* * * * * * *

[SEC. 312. HOMELAND SECURITY INSTITUTE.

[(a) ESTABLISHMENT.—The Secretary shall establish a federally funded research and development center to be known as the "Homeland Security Institute" (in this section referred to as the "Institute").

[(b) ADMINISTRATION.—The Institute shall be administered as a separate entity by the Secretary.

[(c) DUTIES.—The duties of the Institute shall be determined by the Secretary, and may include the following:

[(1) Systems analysis, risk analysis, and simulation and modeling to determine the vulnerabilities of the Nation's critical infrastructures and the effectiveness of the systems deployed to reduce those vulnerabilities.

[(2) Economic and policy analysis to assess the distributed costs and benefits of alternative approaches to enhancing security.

[(3) Evaluation of the effectiveness of measures deployed to enhance the security of institutions, facilities, and infrastructure that may be terrorist targets.

[(4) Identification of instances when common standards and protocols could improve the interoperability and effective utilization of tools developed for field operators and first responders.

[(5) Assistance for Federal agencies and departments in establishing testbeds to evaluate the effectiveness of technologies under development and to assess the appropriateness of such technologies for deployment.

[(6) Design of metrics and use of those metrics to evaluate the effectiveness of homeland security programs throughout the Federal Government, including all national laboratories.

[(7) Design of and support for the conduct of homeland security-related exercises and simulations.

[(8) Creation of strategic technology development plans to reduce vulnerabilities in the Nation's critical infrastructure and key resources.

[(d) CONSULTATION ON INSTITUTE ACTIVITIES.—In carrying out the duties described in subsection (c), the Institute shall consult widely with representatives from private industry, institutions of higher education, nonprofit institutions, other Government agencies, and federally funded research and development centers.

[(e) USE OF CENTERS.—The Institute shall utilize the capabilities of the National Infrastructure Simulation and Analysis Center.

[(f) ANNUAL REPORTS.—The Institute shall transmit to the Secretary and Congress an annual report on the activities of the Institute under this section.

[(g) TERMINATION.—The Homeland Security Institute shall terminate 5 years after its establishment.

[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) 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. 313. OFFICE OF PUBLIC-PRIVATE PARTNERSHIPS.

(a) ESTABLISHMENT OF OFFICE.—There is established an Office of Public-Private Partnerships in the Directorate of Science and Technology.

(b) DIRECTOR.—The Office shall be headed by a Director, who shall be appointed by the Secretary. The Director shall report to the Under Secretary for Science and Technology.

(c) RESPONSIBILITIES.—The Director, in coordination with the Private Sector Office of the Department, shall—

(1) engage and initiate proactive outreach efforts and provide guidance on how to pursue proposals to develop or deploy homeland security technologies (including regarding Federal funding, regulation, or acquisition), including to persons associated with small businesses (as that term is defined in the Small Business Act (15 U.S.C. 631 et seq.));

(2) coordinate with components of the Department to issue announcements seeking unique and innovative homeland security technologies to address homeland security capability gaps;

(3) promote interaction between homeland security researchers and private sector companies in order to accelerate transition research or a prototype into a commercial product and streamline the handling of intellectual property; and

(4) conduct technology research assessment and marketplace analysis for the purpose of identifying, leveraging, and integrating best-of-breed technologies and capabilities from industry, academia, and other Federal Government agencies, and disseminate research and findings to Federal, State, and local governments.

(d) RAPID REVIEW DIVISION.—

(1) ESTABLISHMENT.—There is established the Rapid Review Division within the Office of Public-Private Partnerships.

(2) PURPOSE AND DUTIES.—

(A) IN GENERAL.—The Division—

(i) is responsible for maintaining a capability to perform business and technical reviews to assist in screening unsolicited homeland security technology proposals submitted to the Secretary; and

(ii) shall assess the feasibility, scientific and technical merits, and estimated cost of such proposals.

(B) SPECIFIC DUTIES.—In carrying out those duties, the Division shall—

(i) maintain awareness of the technological requirements of the Directorate's customers;

(ii) establish and publicize accessible, streamlined procedures allowing a participant to have their technology assessed by the Division;

(iii) make knowledgeable assessments of a participant's technology after receiving a business plan, a technology proposal, and a list of corporate officers, directors, and employees with technical knowledge of the proposal, within 60 days after such a submission;

(iv) review proposals submitted by components of the Department to the Division, subject to subsection (e); and

(v) in reviewing proposals submitted to the Secretary, give priority to any proposal submitted by a small business concern as defined under section 3 of the Small Business Act (15 U.S.C. 632).

(3) COORDINATION.—The Director shall submit for consideration promising homeland security technology research, development, testing, and evaluation proposals, along with any business and technical reviews, to the Director of the Homeland Security Advanced Research Projects Agency and appropriate Department components for consideration for support.

(e) LIMITATION ON CONSIDERATION OR EVALUATION OF PROPOSALS.—The Office may not consider or evaluate homeland security technology proposals submitted in response to a solicitation for offers for a pending procurement or for a specific agency requirement.

(f) SATELLITE OFFICES.—The Under Secretary, acting through the Director, may establish up to 3 satellite offices across the country to enhance the Department's outreach efforts. The Secretary shall notify the appropriate congressional committees in writing within 30 days after establishing any satellite office.

(g) PERSONNEL.—The Secretary shall establish rules to prevent the Director or any other employee of the Office from acting on matters where a conflict of interest may exist.

* * * * * * *

SEC. 318. STRATEGIC PLAN.

(a) REQUIREMENT FOR STRATEGIC PLAN.—Not later than 1 year after the date of enactment of this section and every other year thereafter, the Under Secretary for Science and Technology shall prepare a strategic plan for the activities of the Directorate.

(b) CONTENTS.—The strategic plan required by subsection (a) shall be prepared in accordance with applicable Federal requirements, and shall include the following matters:

(1) The long-term strategic goals of the Directorate.

(2) Identification of the research programs of the Directorate that support achievement of those strategic goals.

(3) The connection of the activities and programs of the Directorate to requirements or homeland security capability gaps identified by customers within the Department and outside of the Department, including the first responder community.

(4) The role of the Department's risk analysis in the activities and programs of the Directorate.

(5) A technology transition strategy for the programs of the Directorate.

(6) A description of the policies of the Directorate on the management, organization, and personnel of the Directorate.

(c) SUBMISSION OF PLAN TO CONGRESS.—The Secretary shall submit to Congress any update to the strategic plan most recently prepared under subsection (a) at the same time that the President submits to Congress the budget for each even-numbered fiscal year.

SEC. 319. HOMELAND SECURITY SCIENCE AND TECHNOLOGY FELLOWS PROGRAM.

(a) ESTABLISHMENT.—The Secretary, acting through the Under Secretary for Science and Technology, shall establish a fellows program, to be known as the Homeland Security Science and Technology Fellows Program, under which the Under Secretary shall facilitate the temporary placement of scientists in relevant scientific or technological fields for up to two years in components of the Department with a need for scientific and technological expertise.

(b) UTILIZATION OF FELLOWS.—

(1) IN GENERAL.—Under the Program, the Under Secretary may employ fellows—

(A) for the use of the Directorate of Science and Technology; or

(B) for the use of Department components outside the Directorate, under an agreement with the head of such a component under which the component will reimburse the Directorate for the costs of such employment.

(2) RESPONSIBILITIES.—Under such an agreement—

(A) the Under Secretary shall—

(i) solicit and accept applications from individuals who are currently enrolled in or who are graduates of post-graduate programs in scientific and engineering fields related to the promotion of securing the homeland, including—

(I) biological, chemical, physical, behavioral, social, health, medical, and computational sciences;

(II) geosciences;

(III) all fields of engineering; and

(IV) such other disciplines as are determined relevant by the Secretary;

(ii) screen applicant candidates and interview them as appropriate to ensure that they possess the appropriate level of scientific and engineering expertise and qualifications;

(iii) provide a list of qualified applicants to the heads of Department components seeking to utilize qualified fellows;

(iv) pay financial compensation to such fellows;

(v) coordinate with the Chief Security Officer to facilitate and expedite provision of security clearances to fellows, as appropriate; and

(vi) otherwise administer all aspects of the fellows' employment with the Department; and

(B) the head of the component utilizing the fellow shall—

(i) select a fellow from the list of qualified applicants provided by the Under Secretary;

(ii) reimburse the Under Secretary for the costs of employing the fellow selected; and

(iii) be responsible for the day-to-day management of the fellow.

(c) APPLICATIONS FROM ASSOCIATIONS.—The Under Secretary may accept applications under subsection (b)(2)(A) that are submitted by science or policy associations on behalf of individuals whom such an association has determined may be qualified applicants under the program.

SEC. 320. BIOLOGICAL THREAT AGENT ASSAY EQUIVALENCY PROGRAM.

(a) IN GENERAL.—To facilitate equivalent biological threat agent identification among federally operated biomonitoring programs, the Under Secretary, in consultation with the Director of the Centers for Disease Control and Prevention, may implement an assay equivalency program for biological threat assays.

(b) FEATURES.—In order to establish assay performance equivalency to support homeland security and public health security decisions, the program may—

(1) evaluate biological threat detection assays, their protocols for use, and their associated response algorithms for confirmation of biological threat agents, taking performance measures and concepts of operation into consideration; and

(2) develop assay equivalency standards based on the findings of the evaluation under paragraph (1).

(c) UPDATE.—The Under Secretary shall update the program as necessary.

(d) IMPLEMENTATION.—The Secretary shall—

(1) require implementation of the standards developed under subsection (b)(2) for all Department biomonitoring programs; and

(2) make such standards available to support all other Federal biomonitoring programs.

(e) ASSAY DEFINED.—In this section the term "assay" means any scientific test that is—

(1) designed to detect the presence of a biological threat agent; and

(2) of a type selected under criteria established by the Secretary.

* * * * * * *

TITLE VIII—COORDINATION WITH NON-FEDERAL ENTITIES; INSPECTOR GENERAL; UNITED STATES SECRET SERVICE; COAST GUARD; GENERAL PROVISIONS

* * * * * * *

Subtitle D—Acquisitions

SEC. 831. RESEARCH AND DEVELOPMENT PROJECTS.

(a) AUTHORITY.—Until September 30, [2010,] *2012,* and subject to subsection (d), the Secretary may carry out a pilot program under which the Secretary may exercise the following authorities:

(1)* * *

* * * * * * *

(3) PRIOR APPROVAL.—In any case in which the Under Secretary for Science and Technology intends to exercise other transaction authority, the Under Secretary must receive prior approval from the Secretary after submitting to the Secretary a proposal that includes the rationale for why a grant or contract issued in accordance with the Federal Acquisition Regulation is not feasible or appropriate and the amount to be expended for such project. In such a case, the authority for evaluating the proposal may not be delegated by the Secretary to anyone other than the Under Secretary for Management.

* * * * * * *

(e) ANNUAL REPORT ON EXERCISE OF OTHER TRANSACTION AUTHORITY.—

(1) IN GENERAL.—The Secretary shall submit to the appropriate congressional committees an annual report on the exercise of other transaction authority.

(2) CONTENT.—The report shall include the following:

(A) The subject areas in which research projects were conducted using other transaction authority.

(B) The extent of cost-sharing for such projects among Federal and non-Federal sources.

(C) The extent to which use of other transaction authority has addressed a homeland security capability gap identified by the Department of Homeland Security.

(D) The total amount of payments, if any, that were received by the Federal Government as a result of such exer-

cise of other transaction authority during the period covered by the report.

(E) The rationale for using other transaction authority, including why grants or contracts issued in accordance with the Federal Acquisition Regulation were not feasible or appropriate.

(F) the amount expended for each such project.

(f) TRAINING.—The Secretary shall develop a training program for acquisitions staff in the use of other transaction authority to help ensure the appropriate use of such authority.

(g) REVIEW AUTHORITY.—The exercise of other transaction authority shall be subject to review by the Comptroller General of the United States to ensure that an agency is not attempting to avoid the requirements of procurement statutes and regulations.

(h) OTHER TRANSACTION AUTHORITY DEFINED.—In this section the term "other transaction authority" means authority under subsection (a).

[(e)**]** *(i)* DEFINITION OF NONTRADITIONAL GOVERNMENT CONTRACTOR.—In this section, the term "nontraditional Government contractor" has the same meaning as the term "nontraditional defense contractor" as defined in section 845(e) of the National Defense Authorization Act for Fiscal Year 1994 (Public Law 103–160; 10 U.S.C. 2371 note).

* * * * * * *

○