111TH CONGRESS
2D SESSION

H. R. 4842

IN THE SENATE OF THE UNITED STATES

JULY 21, 2010

Received; read twice and referred to the Committee on Homeland Security and Governmental Affairs

AN ACT

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.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

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

and the Committee on Science and Technology 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.—Title III (6 U.S.C. 181 et seq.) is amended by adding at the end the following new sections:

"SEC. 318. RESEARCH PRIORITIZATION AND REQUIREMENTS.

''(a) REQUIREMENTS.—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, the Director of the Domestic Nuclear Detection Office, 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, including the risk assessment required under subsection (e)(1) 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, including 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; and

''(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;

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

''(7) 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) carry out the requirements of subsection (a);

''(2) 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 319(a)(2);

''(3) establish a system to collect feedback from customers of the Directorate on the performance of the Directorate; and

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

''(d) BIANNUAL UPDATES ON IMPLEMENTATION.—One hundred and eighty days after the date of enactment of this section, and on a biannually basis thereafter, the Inspector General of the Department shall submit a biannually 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 ASSESSMENT.—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 carried out by the Secretary, 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 assessment;

''(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, as appropriate;

''(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, as appropriate;

''(D) 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, including recommendations for how the Directorate should modify or amend its existing research and development activities, including for purposes of reducing the risks to the homeland identified under subparagraph (A); and

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

''(2) conduct research and development on ways to most effectively communicate information regarding the risks identified under paragraph (1)(A) 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, as appropriate, the corresponding risk identified in subsection (e)(1)(A) that supports the decision to undertake that activity; and

''(B) describe any 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. 319. PROFESSIONAL DEVELOPMENT.

''(a) REPORTING REQUIREMENT.—Sixty days before establishing the mandatory workforce program as required by section 318(c)(2), 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) A description of the training that should be provided to the Directorate's customers in the Department under the mandatory workforce program 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 318(c)(2), 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. 320. CUSTOMER FEEDBACK.

''In establishing a system to collect feedback under section 318(c)(3), the Secretary shall—

''(1) 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;

''(2) develop metrics for measuring customer satisfaction and the usefulness of any technology or service provided by the Directorate; and

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

''SEC. 321. RESEARCH PROGRESS.

''(a) IN GENERAL.—The Secretary shall establish a system to monitor the progress of Directorate for Science and Technology research, development, testing, and evaluation activities, including the establishment of initial and subsequent research milestones.

''(b) SYSTEM.—The system established under subsection (a) shall—

''(1) identify and monitor the progress toward research milestones;

''(2) allow the Directorate to provide regular reports to its customers regarding the status and progress of research efforts of the Directorate;

''(3) allow 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) allow 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 on setting valid initial and subsequent research milestones for homeland security research funded by the Directorate.

''SEC. 322. REPORT.

''(a) IN GENERAL.—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 sections 320 and 321 identifying what actions have been taken to carry out the requirements of these sections; and

''(2) annually thereafter describing—

''(A) research milestones for each large project with a Federal cost share greater than $80,000,000 that have 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. 318. Research prioritization and requirements.
''Sec. 319. Professional development.
''Sec. 320. Customer feedback.
''Sec. 321. Research progress.
''Sec. 322. Report.

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 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 Department's use of technical standards that are developed or adopted by voluntary consensus standards bodies 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. EXTERNAL 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 periodic external review of research and development programs or activities, including through—

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

''(B) ongoing independent, external 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 programs or activities are subject to external review, 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 Di-

rector 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 partici-

pant 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 appropriate subcomponents of the Directorate and the appropriate operational components of the Department 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.), as amended by section 201, is further amended by adding at the end the following new section:

"SEC. 323. 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), as amended by section 201, is further amended by adding at the end of the items relating to title III the following new item:

''Sec. 323. 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, the Under Secretary shall, for

each current project conducted by the Directorate and having a Federal cost share greater than $80,000,000, and on an ongoing basis thereafter for any new project conducted by the Directorate and having a Federal cost share greater than $80,000,000, provide to the appropriate congressional committees a description of—

''(A) the Department components and customers consulted during the development of the operational and technical requirements associated with the project; and

''(B) the extent to which the requirements incorporate the input of those components or customers.

''(2) LARGE PROJECTS.—Within 90 days after the date of enactment, the Secretary shall, for each current project conducted by a component of the Department besides the Directorate, and having a life-cycle cost greater than $1,000,000,000, and on an ongoing basis thereafter for any new project conducted by a component of the Department besides the Directorate, and 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 to be appropriated $500,000 for the report under this section.

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 the Department's efforts to identify key areas of study needed to support the homeland security mission, and criteria that the Department 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 best practices from other agencies efforts to organize and use university-based research to support their missions.

(5) A review of the Department's 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 Secu-

rity 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 pro-

vision 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 periodically conduct research to 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 differen-

tiate 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 con-

gressional 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 de-

tection 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 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 com-

plement 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 capac-

ity 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 the National Institute of Standards and Technology and any 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. 324. 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 graduate programs, or have received a graduate degree within 3 years prior to the time of application 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. 324. 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. 325. 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 other relevant Federal agencies, 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. 325. 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.

''(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.

SEC. 422. HOMELAND SECURITY SCIENCE AND TECHNOLOGY ADVISORY COMMITTEE.

Section 301 of the Homeland Security Act of 2002 (6 U.S.C. 191) is amended—

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

''(a) There is established within the Department a science and technology advisory committee (in this section referred to as the 'advisory committee'). The advisory

committee shall make recommendations with respect to the activities of the under secretary for science and technology, including—

''(1) identifying research areas of potential importance to the security of the Nation; and

''(2) providing advice in developing and updating the strategic plan required under section 318.''.

(2) by striking subsection (j).

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, the Under Secretary, and the heads of all operational components of the Department that own, operate, or maintain nuclear or radiological detection equipment shall begin an internal review of the methodology by which research, development, testing, and evaluation is identified, prioritized, and funded within the Department.

(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 Direc-

tor 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 Government wide 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 De-

partment 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 one year 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, com-

pared to other Department of Energy national laboratory work performed for the Department on a ''work for others'' basis.

(4) Review the cost savings identified by 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.

SEC. 604. TECHNICAL CHANGES.

Section 1902 of the Homeland Security Act (6 U.S.C. 592) is amended by—

(1) striking paragraph (6); and

(2) redesignating paragraphs (7) through (14) as paragraphs (6) through (13), respectively.

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 Elec-

tronic 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 have 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.

TITLE VIII—BORDER SECURITY TECHNOLOGY INNOVATION

SEC. 801. ENSURING RESEARCH ACTIVITIES OF THE DEPARTMENT OF HOMELAND SECURITY INCLUDE APPROPRIATE CONCEPTS OF OPERATION.

The Under Secretary shall ensure that any Federal Government interagency or intra-agency agreement entered into by the Under Secretary to develop and transition new technology explicitly characterizes the requirements, expected use, and concept of operations for that technology, including—

(1) the manpower needed to effectively operate the technology;

(2) the expected training requirements; and

(3) the expected operations and maintenance costs.

SEC. 802. REPORT ON BASIC RESEARCH NEEDS FOR BORDER AND MARITIME SECURITY.

Not later than 6 months after the date of enactment of this Act, the Under Secretary shall enter into an arrangement with the National Research Council for a one-year assessment of the basic science research needs in the

border and maritime security domain. The assessment shall include consideration of—

(1) detection, tracking, and identification technologies for cargo and people;

(2) personal protective equipment;

(3) document security and authentication technologies;

(4) nonradiological advanced screening technologies at ports of entry; and

(5) technologies for real time tactical scene awareness.

SEC. 803. INCORPORATING UNMANNED AERIAL VEHICLES INTO BORDER AND MARITIME AIRSPACE.

(a) RESEARCH AND DEVELOPMENT.—The Secretary and the Director of the Joint Planning and Development Office shall research and develop technologies to permit routine operation of unmanned aerial vehicles, including autonomously piloted drones, within the national airspace for border and maritime security missions without any degradation of existing levels of safety for all national airspace system users.

(b) PILOT PROJECTS.—The Secretary shall coordinate with the Administrator of the Federal Aviation Administration and the Director of the Joint Planning Office to enter into pilot projects in sparsely populated, low-den-

sity Class G air traffic airspace to conduct experiments and collect data in order to accelerate the safe integration of unmanned aircraft systems into the national airspace system as part of research activities of the Joint Planning and Development Office.

SEC. 804. ESTABLISHING A RESEARCH PROGRAM IN TUNNEL DETECTION.

(a) RESEARCH AND DEVELOPMENT.—The Under Secretary shall research and develop technologies to permit detection of near surface voids, such as tunnels, with an emphasis on technologies with real time capability.

(b) COORDINATION.—The Secretary shall coordinate with other appropriate Federal agencies, including the Department of Defense and the United States Geological Survey, and ensure the integration of activities under subsection (a) with relevant efforts of such other agencies and the Department's Centers of Excellence Program.

SEC. 805. RESEARCH IN DOCUMENT SECURITY AND AUTHENTICATION TECHNOLOGIES.

(a) ESTABLISHMENT OF PROGRAM.—The Under Secretary, in coordination with the Director of the National Institute of Standards and Technology, shall conduct a research and development program on document security, validation, and authentication technologies and standards. The program may include assessment or development of

imitation-resistant and tamper-resistant documentation, imitation-resistant or tamper-resistant devices, document validation and authentication technologies, and document identification standards.

(b) COORDINATION.—In carrying out the program in subsection (a), the Under Secretary shall coordinate with other Federal agencies engaged in similar activities, including Immigration and Customs Enforcement, the Department of State, the Department of Defense, the United States Coast Guard, and the Department of Justice.

(c) REPORT TO CONGRESS.—Not later than 12 months after the date of enactment of this Act, the Under Secretary and the Director of the National Institute of Standards and Technology shall provide to the Committee on Homeland Security and the Committee on Science and Technology of the House of Representatives, and the Committee on Homeland Security and Government Affairs of the Senate, a report detailing the actions taken by the Under Secretary and the Director under this section.

SEC. 806. STUDY ON GLOBAL POSITIONING SYSTEM TECHNOLOGIES.

(a) IN GENERAL.—The Under Secretary shall conduct a study of the need for next generation global positioning system technology as it relates to border security, including—

(1) conducting an analysis of the frequency of unintended border crossings and the capability of global positioning system technologies to address unintended border crossings by government personnel;

(2) undertaking an examination of the potential end user requirements for global positioning system technologies, including cost limitations, accessibility, and reliability; and

(3) developing recommendations for potential near-term and long-term research, development, testing, and evaluation of border security-focused global positioning technologies.

(b) CONSULTATION.—In conducting the study under subsection (a), the Under Secretary shall consult with U.S. Customs and Border Protection, the National Institute of Standards and Technology and appropriate Federal, State, and local law enforcement officials.

(c) REPORT.—Not later than 1 year after the date of enactment of this Act, the Under Secretary shall report to Congress the findings of the study conducted under this section.

SEC. 807. STUDY OF MOBILE BIOMETRIC TECHNOLOGIES AT THE BORDER.

(a) IN GENERAL.—The Under Secretary, in coordination with the Commissioner of United States Customs

and Border Protection, shall establish a research program on the use of mobile biometric technology at the Nation's borders between the ports of entry, including—

(1) conducting an analysis of existing mobile biometric technologies and the extent to which they can be deployed in Border Patrol agents' vehicles and used at the border, in terms of operability, reliability, cost, and overall benefit to border operations;

(2) undertaking an examination of the potential end-user requirements of mobile biometric technology by the Border Patrol and other relevant end-users;

(3) developing recommendations for addressing capability gaps in mobile biometric technologies; and

(4) examining the feasibility of implementing a pilot program for use of mobile biometric technologies at the border.

(b) CONSULTATION.—In conducting the research program under subsection (a), the Under Secretary shall consult the National Institute of Standards and Technology, other appropriate Federal agencies, and appropriate Federal, State, and local law enforcement officials.

(c) COORDINATION.—The Secretary shall ensure that the research program is coordinated with other biometric identification programs within the Department.

(d) REPORT.—Not later than 6 months after the date of enactment of this Act, the Under Secretary shall transmit to Congress a report on the findings of the research program conducted under this section.

SEC. 808. AUTHORIZATION OF APPROPRIATIONS.

Of the amount authorized by section 101 of this Act, such sums as may be necessary are authorized to be appropriated to carry out this title.

Passed the House of Representatives July 20, 2010.

Attest: LORRAINE C. MILLER,

Clerk.