AMENDMENT TO RULES COMM. PRINT 117–54
OFFERED BY MR. THOMPSON OF MISSISSIPPI

Add at the end of division E the following:

TITLE LIX—HOMELAND
SECURITY PROVISIONS
Subtitle A—Strengthening Security of Our Communities
SEC. 59101. NONPROFIT SECURITY GRANT PROGRAM IMPROVEMENT.
   (a) In General.—Section 2009 of the Homeland Security Act of 2002 (6 U.S.C. 609a) is amended—
   (1) in subsection (a), by inserting “and threats” before the period at the end;
   (2) in subsection (b)—
   (A) in the matter preceding paragraph (1), by striking “this subsection (a)” and inserting “this subsection”; and
   (B) by amending paragraph (2) to read as follows:
   “(2) determined by the Secretary to be at risk of terrorist attacks and threats.”;
   (3) in subsection (c)—
(A) by redesignating paragraphs (1), (2),
and (3) as subparagraphs (A), (B), and (E), re-
spectively, and moving such subparagraphs, as
so redesignated, two ems to the right;

(B) in the matter preceding subparagraph
(A), as so redesignated, by striking “The recipi-
ent” and inserting the following:
“(1) IN GENERAL.—The recipient”;  

(C) in subparagraph (A), as so redesig-
nated, by striking “equipment and inspection
and screening systems” and inserting “equip-
ment, inspection and screening systems, and al-
teration or remodeling of existing buildings or
physical facilities”;

(D) by inserting after subparagraph (B),
as so redesignated, the following new subpara-
graphs:
“(C) Facility security personnel costs, in-
cluding costs associated with contracted secu-

(D) Expenses directly related to the ad-
ministration of the grant, except that such ex-

amount of the grant.”; and
(E) by adding at the end the following new paragraph:

“(2) RETENTION.—Each State through which a recipient receives a grant under this section may retain up to five percent of each grant for expenses directly related to the administration of the grant.”;

(4) in subsection (e)—

(A) by striking “2020 through 2024” and inserting “2022 through 2028”; and

(B) by adding at the end the following new sentence: “Each such report shall also include information on the number of applications submitted by eligible nonprofit organizations to each State, the number of applications submitted by each State to the Administrator, and the operations of the Nonprofit Security Grant Program Office, including staffing resources and efforts with respect to subparagraphs (A) through (E) of subsection (c)(1).”;

(5) by redesignating subsection (f) as subsection (j);

(6) by inserting after subsection (e) the following new subsections:

“(f) ADMINISTRATION.—Not later than 120 days after the date of the enactment of this subsection, the Ad-
Administrator shall establish within the Federal Emergency Management Agency a program office for the Program (in this section referred to as the ‘program office’). The program office shall be headed by a senior official of the Agency. The Administrator shall administer the Program (including, where appropriate, in coordination with States), including relating to the following:

“(1) Outreach, engagement, education, and technical assistance and support to eligible nonprofit organizations described in subsection (b), with particular attention to such organizations in underserved communities, prior to, during, and after the awarding of grants, including web-based training videos for eligible nonprofit organizations that provide guidance on preparing an application and the environmental planning and historic preservation process.

“(2) Establishment of mechanisms to ensure program office processes are conducted in accordance with constitutional, statutory, regulatory, and other legal and agency policy requirements that protect civil rights and civil liberties and, to the maximum extent practicable, advance equity for members of underserved communities.
“(3) Establishment of mechanisms for the Administrator to provide feedback to eligible nonprofit organizations that do not receive grants.

“(4) Establishment of mechanisms to collect data to measure the effectiveness of grants under the Program.

“(5) Establishment and enforcement of standardized baseline operational requirements for States, including requirements for States to eliminate or prevent any administrative or operational obstacles that may impact eligible nonprofit organizations described in subsection (b) from receiving grants under the Program.

“(6) Carrying out efforts to prevent waste, fraud, and abuse, including through audits of grantees.

“(g) GRANT GUIDELINES.—For each fiscal year, prior to awarding grants under this section, the Administrator—

“(1) shall publish guidelines, including a notice of funding opportunity or similar announcement, as the Administrator determines appropriate; and

“(2) may prohibit States from closing application processes prior to the publication of such guidelines.
“(h) ALLOCATION REQUIREMENTS.—

“(1) IN GENERAL.—In awarding grants under this section, the Administrator shall ensure that—

“(A) 50 percent of amounts appropriated pursuant to the authorization of appropriations under subsection (k) is provided to eligible recipients located in high-risk urban areas that receive funding under section 2003 in the current fiscal year or received such funding in any of the preceding ten fiscal years, inclusive of any amounts States may retain pursuant to paragraph (2) of subsection (c); and

“(B) 50 percent of amounts appropriated pursuant to the authorizations of appropriations under subsection (k) is provided to eligible recipients located in jurisdictions not receiving funding under section 2003 in the current fiscal year or have not received such funding in any of the preceding ten fiscal years, inclusive of any amounts States may retain pursuant to paragraph (2) of subsection (c).

“(2) EXCEPTION.—Notwithstanding paragraph (1), the Administrator may allocate a different percentage if the Administrator does not receive a sufficient number of applications from eligible recipients
to meet the allocation percentages described in either subparagraph (A) or (B) of such paragraph. If the Administrator exercises the authorization under this paragraph, the Administrator shall, not later than 30 days after such exercise, report to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate regarding such exercise.

“(i) PAPERWORK REDUCTION ACT.—Chapter 35 of title 44, United States Code (commonly known as the ‘Paperwork Reduction Act’), shall not apply to any changes to the application materials, Program forms, or other core Program documentation intended to enhance participation by eligible nonprofit organizations in the Program.”;

(7) in subsection (j), as so redesignated—

(A) in paragraph (1), by striking “$75 million for each of fiscal years 2020 through 2024” and inserting “$75,000,000 for fiscal year 2023 and $500,000,000 for each of fiscal years 2024 through 2028”; and

(B) by amending paragraph (2) to read as follows:

“(2) OPERATIONS AND MAINTENANCE.—Of the amounts authorized to be appropriated pursuant to
paragraph (1), not more than five percent is author-
ized—

“(A) to operate the program office; and

“(B) for other costs associated with the
management, administration, and evaluation of
the Program.”; and

(8) by adding at the end the following new sub-
section:

“(k) TREATMENT.—Nonprofit organizations deter-
mined by the Secretary to be at risk of extremist attacks
other than terrorist attacks and threats under subsection
(a) are deemed to satisfy the conditions specified in sub-
section (b) if protecting such organizations against such
other extremist attacks would help protect such organiza-
tions against such terrorist attacks and threats.”.

(b) PLAN.—Not later than 90 days after the date of
the enactment of this Act, the Administrator of the Fed-
eral Emergency Management Agency shall submit to the
Committee on Homeland Security of the House of Rep-
resentatives and the Committee on Homeland Security
and Governmental Affairs of the Senate a plan for the
administration of the program office for the Nonprofit Se-
curity Grant Program established under subsection (f) of
section 2009 of the Homeland Security Act 2002 (6
U.S.C. 609a), as amended by subsection (a), including a staffing plan for such program office.

(c) CONFORMING AMENDMENT.—Section 2008 of the Homeland Security Act of 2002 (6 U.S.C. 609) is amended—

(1) in subsection (c) by striking “sections 2003 and 2004” and inserting “sections 2003, 2004, and 2009”; and

(2) in subsection (e), by striking “section 2003 or 2004” and inserting “sections 2003, 2004, or 2009”.

SEC. 59102. NATIONAL COMPUTER FORENSICS INSTITUTE REAUTHORIZATION.

(a) IN GENERAL.—Section 822 of the Homeland Security Act of 2002 (6 U.S.C. 383) is amended—

(1) in subsection (a)—

(A) in the subsection heading, by striking “IN GENERAL” and inserting “IN GENERAL; MISSION”;

(B) by striking “2022” and inserting “2032”; and

(C) by striking the second sentence and inserting “The Institute’s mission shall be to educate, train, and equip State, local, territorial, and Tribal law enforcement officers, prosecu-
tors, judges, participants in the United States Secret Service’s network of cyber fraud task forces, and other appropriate individuals regarding the investigation and prevention of cybersecurity incidents, electronic crimes, and related cybersecurity threats, including through the dissemination of homeland security information, in accordance with relevant Department guidance regarding privacy, civil rights, and civil liberties protections.”;

(2) by redesignating subsections (c) through (f) as subsections (d) through (g), respectively;

(3) by striking subsection (b) and inserting the following new subsections:

“(b) CURRICULUM.—In furtherance of subsection (a), all education and training of the Institute shall be conducted in accordance with relevant Federal law and policy regarding privacy, civil rights, and civil liberties protections, including best practices for safeguarding data privacy and fair information practice principles. Education and training provided pursuant to subsection (a) shall relate to the following:

“(1) Investigating and preventing cybersecurity incidents, electronic crimes, and related cybersecurity threats, including relating to instances involving
illicit use of digital assets and emerging trends in cyber
security and electronic crime.

“(2) Conducting forensic examinations of computers, mobile devices, and other information systems.

“(3) Prosecutorial and judicial considerations related to cybersecurity incidents, electronic crimes, related cybersecurity threats, and forensic examinations of computers, mobile devices, and other information systems.

“(4) Methods to obtain, process, store, and admit digital evidence in court.

“(c) RESEARCH AND DEVELOPMENT.—In furtherance of subsection (a), the Institute shall research, develop, and share information relating to investigating cybersecurity incidents, electronic crimes, and related cybersecurity threats that prioritize best practices for forensic examinations of computers, mobile devices, and other information systems. Such information may include training on methods to investigate ransomware and other threats involving the use of digital assets.”;

(4) in subsection (d), as so redesignated—

(A) by striking “cyber and electronic crime and related threats is shared with State, local, tribal, and territorial law enforcement officers
and prosecutors” and inserting “cybersecurity incidents, electronic crimes, and related cybersecurity threats is shared with recipients of education and training provided pursuant to subsection (a)”; and

(B) by adding at the end the following new sentence: “The Institute shall prioritize providing education and training to individuals from geographically-diverse jurisdictions throughout the United States.”;

(5) in subsection (e), as so redesignated—

(A) by striking “State, local, tribal, and territorial law enforcement officers” and inserting “recipients of education and training provided pursuant to subsection (a)”; and

(B) by striking “necessary to conduct cyber and electronic crime and related threat investigations and computer and mobile device forensic examinations” and inserting “for investigating and preventing cybersecurity incidents, electronic crimes, related cybersecurity threats, and for forensic examinations of computers, mobile devices, and other information systems”;

(6) in subsection (f), as so redesignated—
(A) by amending the heading to read as follows: “CYBER FRAUD TASK FORCES”;

(B) by striking “Electronic Crime” and inserting “Cyber Fraud”;

(C) by striking “State, local, tribal, and territorial law enforcement officers” and inserting “recipients of education and training provided pursuant to subsection (a)”; and

(D) by striking “at” and inserting “by”;

(7) by redesignating subsection (g), as redesignated pursuant to paragraph (2), as subsection (j); and

(8) by inserting after subsection (f), as so redesignated, the following new subsections:

“(g) EXPENSES.—The Director of the United States Secret Service may pay for all or a part of the education, training, or equipment provided by the Institute, including relating to the travel, transportation, and subsistence expenses of recipients of education and training provided pursuant to subsection (a).

“(h) ANNUAL REPORTS TO CONGRESS.—The Secretary shall include in the annual report required pursuant to section 1116 of title 31, United States Code, information regarding the activities of the Institute, including relating to the following:
“(1) Activities of the Institute, including, where possible, an identification of jurisdictions with recipients of education and training provided pursuant to subsection (a) of this section during such year and information relating to the costs associated with such education and training.

“(2) Any information regarding projected future demand for such education and training.

“(3) Impacts of the Institute’s activities on jurisdictions’ capability to investigate and prevent cybersecurity incidents, electronic crimes, and related cybersecurity threats.

“(4) A description of the nomination process for State, local, territorial, and Tribal law enforcement officers, prosecutors, judges, participants in the United States Secret Service’s network of cyber fraud task forces, and other appropriate individuals to receive the education and training provided pursuant to subsection (a).

“(5) Any other issues determined relevant by the Secretary.

“(i) DEFINITIONS.—In this section—

“(1) CYBERSECURITY THREAT.—The term ‘cybersecurity threat’ has the meaning given such term in section 102 of the Cybersecurity Act of 2015 (en-
acted as division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113; 6 U.S.C. 1501))

“(2) INCIDENT.—The term ‘incident’ has the meaning given such term in section 2209(a).

“(3) INFORMATION SYSTEM.—The term ‘information system’ has the meaning given such term in section 102 of the Cybersecurity Act of 2015 (enacted as division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113; 6 U.S.C. 1501(9))).”.

(b) GUIDANCE FROM THE PRIVACY OFFICER AND CIVIL RIGHTS AND CIVIL LIBERTIES OFFICER.—The Privacy Officer and the Officer for Civil Rights and Civil Liberties of the Department of Homeland Security shall provide guidance, upon the request of the Director of the United States Secret Service, regarding the functions specified in subsection (b) of section 822 of the Homeland Security Act of 2002 (6 U.S.C. 383), as amended by subsection (a).

(c) TEMPLATE FOR INFORMATION COLLECTION FROM PARTICIPATING JURISDICTIONS.—Not later than 180 days after the date of the enactment of this Act, the Director of the United States Secret Service shall develop and disseminate to jurisdictions that are recipients of edu-
cation and training provided by the National Computer Forensics Institute pursuant to subsection (a) of section 822 of the Homeland Security Act of 2002 (6 U.S.C. 383), as amended by subsection (a), a template to permit each such jurisdiction to submit to the Director reports on the impacts on such jurisdiction of such education and training, including information on the number of digital forensics exams conducted annually. The Director shall, as appropriate, revise such template and disseminate to jurisdictions described in this subsection any such revised templates.

(d) REQUIREMENTS ANALYSIS.—

(1) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Director of the United States Secret Service shall carry out a requirements analysis of approaches to expand capacity of the National Computer Forensics Institute to carry out the Institute’s mission as set forth in subsection (a) of section 822 of the Homeland Security Act of 2002 (6 U.S.C. 383), as amended by subsection (a).

(2) SUBMISSION.—Not later than 90 days after completing the requirements analysis under paragraph (1), the Director of the United States Secret Service shall submit to Congress such analysis, to-
together with a plan to expand the capacity of the Na-
tional Computer Forensics Institute to provide edu-
cation and training described in such subsection.

Such analysis and plan shall consider the following:

(A) Expanding the physical operations of
the Institute.

(B) Expanding the availability of virtual
education and training to all or a subset of po-
tential recipients of education and training from
the Institute.

(C) Some combination of the consider-
ations set forth in subparagraphs (A) and (B).

(e) RESEARCH AND DEVELOPMENT.—The Director
of the United States Secret Service may coordinate with
the Under Secretary for Science and Technology of the
Department of Homeland Security to carry out research
and development of systems and procedures to enhance
the National Computer Forensics Institute’s capabilities
and capacity to carry out the Institute’s mission as set
forth in subsection (a) of section 822 of the Homeland
Security Act of 2002 (6 U.S.C. 383), as amended by sub-
section (a).

SEC. 59103. HOMELAND SECURITY CAPABILITIES PRESER-
VATION.

(a) PLAN.—
(1) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Secretary of Homeland Security, acting through the Administrator of the Federal Emergency Management Agency, shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a plan, informed by the survey information collected pursuant to subsection (b), to make Federal assistance available for at least three consecutive fiscal years to certain urban areas that in the current fiscal year did not receive grant funding under the Urban Area Security Initiative under section 2003 of the Homeland Security Act of 2002 (6 U.S.C. 604) and require continued Federal assistance for the purpose of preserving a homeland security capability related to preventing, preparing for, protecting against, and responding to acts of terrorism that had been developed or otherwise supported through prior grant funding under such Initiative and allow for such urban areas to transition to such urban areas costs of preserving such homeland security capabilities.

(2) ADDITIONAL REQUIREMENT.—The plan required under paragraph (1) shall also contain a pro-
hition on an urban area that in a fiscal year is eli-
gible to receive Federal assistance described in such
paragraph from also receiving grant funding under
the Urban Area Security Initiative under section
a case, such plan shall require such an urban area
to promptly notify the Administrator of the Federal
Emergency Management Agency regarding the pref-
ference of such urban area to retain either—

(A) such eligibility for such Federal assist-
ance; or

(B) such receipt of such grant funding.

(b) SURVEY.—In developing the plan required under
subsection (a), the Administrator of the Federal Emer-
gency Management Agency, shall, to ascertain the scope
of Federal assistance required, survey urban areas that—

(1) did not receive grant funding under the
Urban Area Security Initiative under section 2003
of the Homeland Security Act of 2002 in the current
fiscal year concerning homeland security capabilities
related to preventing, preparing for, protecting
against, and responding to acts of terrorism that
had been developed or otherwise supported through
funding under such Initiative that are at risk of
being reduced or eliminated without such Federal assistance;

(2) received such funding in the current fiscal year, but did not receive such funding in at least one fiscal year in the six fiscal years immediately preceding the current fiscal year; and

(3) any other urban areas the Secretary determines appropriate.

(e) EXEMPTION.—The Secretary of Homeland Security may exempt the Federal Emergency Management Agency from the requirements of subchapter I of chapter 35 of title 44, United States Code (commonly referred to as the “Paperwork Reduction Act’’), for purposes of carrying out subsection (b) if the Secretary determines that complying with such requirements would delay the development of the plan required under subsection (a).

(d) CONTENTS.—The plan required under subsection (a) shall—

(1) establish eligibility criteria for urban areas to receive Federal assistance pursuant to such plan to provide assistance for the purpose described in such subsection;

(2) identify annual funding levels for such Federal assistance in accordance with the survey required under subsection (b); and
(3) consider a range of approaches to make
such Federal assistance available to such urban
areas, including—

(A) modifications to the Urban Area Secu-

rity Initiative under section 2003 of the Home-

land Security Act of 2002 in a manner that

would not affect the availability of funding to

urban areas under such Initiative;

(B) the establishment of a competitive

grant program;

(C) the establishment of a formula grant

program; and

(D) a timeline for the implementation of

any such approach and, if necessary, a legisla-
tive proposal to authorize any such approach.

SEC. 59104. SCHOOL AND DAYCARE PROTECTION.

(a) IN GENERAL.—Title VII of the Homeland Secu-

rity Act of 2002 (6 U.S.C. 341 et seq.) is amended by

adding at the end the following new section:

“SEC. 714. SCHOOL SECURITY COORDINATING COUNCIL.

“(a) ESTABLISHMENT.—There is established in the

Department a coordinating council to ensure that, to the

maximum extent practicable, activities, plans, and policies

to enhance the security of early childhood education pro-
grams, elementary schools, high schools, and secondary
schools against acts of terrorism and other homeland security threats are coordinated.

“(b) COMPOSITION.—The members of the council established pursuant to subsection (a) shall include the following:

“(1) The Under Secretary for Strategy, Policy, and Plans.

“(2) The Director of the Cybersecurity and Infrastructure Security.


“(4) The Director of the Secret Service.

“(5) The Executive Director of the Office of Academic Engagement.

“(6) The Assistant Secretary for Public Affairs.

“(7) Any other official of the Department the Secretary determines appropriate.

“(c) LEADERSHIP.—The Secretary shall designate a member of the council to serve as chair of the council.

“(d) RESOURCES.—The Secretary shall participate in Federal efforts to maintain and publicize a clearinghouse of resources available to early childhood education programs, elementary schools, high schools, and secondary schools to enhance security against acts of terrorism and other homeland security threats.
“(e) REPORTS.—Not later than January 30, 2023, and annually thereafter, the Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report regarding the following:

“(1) The Department’s activities, plans, and policies aimed at enhancing the security of early childhood education programs, elementary schools, high schools, and secondary schools against acts of terrorism and other homeland security threats.

“(2) With respect to the immediately preceding year, information on the following:

“(A) The council’s activities during such year.

“(B) The Department’s contributions to Federal efforts to maintain and publicize the clearinghouse of resources referred to in subsection (d) during such year.

“(3) Any metrics regarding the efficacy of such activities and contributions, and any engagement with stakeholders outside of the Federal Government.

“(f) DEFINITIONS.—In this section, the terms ‘early childhood education program’, ‘elementary school’, ‘high
school', and ‘secondary school’ have the meanings given such terms in section 8101 of the Elementary and Sec-
ondary Education Act of 1965 (20 U.S.C. 7801).”.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is
amended by inserting after the item relating to section
713 the following new item:

“Sec. 714. School security coordinating council.”.

SEC. 59105. REPORTING EFFICIENTLY TO PROPER OFFI-
CIALS IN RESPONSE TO TERRORISM.

(a) IN GENERAL.—Whenever an act of terrorism oc-
curs in the United States, the Secretary of Homeland Se-
curity, the Attorney General, the Director of the Federal
Bureau of Investigation, and, as appropriate, the head of
the National Counterterrorism Center, shall submit to the
appropriate congressional committees, by not later than
one year after the completion of the investigation con-
cerning such act by the primary Government agency con-
ducting such investigation, an unclassified report (which
may be accompanied by a classified annex) concerning
such act.

(b) CONTENT OF REPORTS.—A report under this sec-
tion shall—

(1) include a statement of the facts of the act
of terrorism referred to in subsection (a), as known
at the time of the report;
(2) identify any gaps in homeland or national security that could be addressed to prevent future acts of terrorism; and

(3) include any recommendations for additional measures that could be taken to improve homeland or national security, including recommendations relating to potential changes in law enforcement practices or changes in law, with particular attention to changes that could help prevent future acts of terrorism.

(c) EXCEPTION.—

(1) IN GENERAL.—If the Secretary of Homeland Security, the Attorney General, the Director of the Federal Bureau of Investigation, or, as appropriate, the head of the National Counterterrorism Center determines any information described in subsection (b) required to be reported in accordance with subsection (a) could jeopardize an ongoing investigation or prosecution, the Secretary, Attorney General, Director, or head, as the case may be—

(A) may withhold from reporting such information; and

(B) shall notify the appropriate congressional committees of such determination.
(2) Saving provision.—Withholding of information pursuant to a determination under paragraph (1) shall not affect in any manner the responsibility to submit a report required under subsection (a) containing other information described in subsection (b) not subject to such determination.

(d) Definitions.—In this section:

(1) Act of terrorism.—The term “act of terrorism” has the meaning given such term in section 3077 of title 18, United States Code.

(2) Appropriate congressional committees.—The term “appropriate congressional committees” means—

(A) in the House of Representatives—

(i) the Committee on Homeland Security;

(ii) the Committee on the Judiciary; and

(iii) the Permanent Select Committee on Intelligence; and

(B) in the Senate—

(i) the Committee on Homeland Security and Governmental Affairs;

(ii) the Committee on the Judiciary; and
(iii) the Select Committee on Intelligence.

SEC. 59106. CYBERSECURITY GRANTS FOR SCHOOLS.

(a) IN GENERAL.—Section 2220 of the Homeland Security Act of 2002 (6 U.S.C. 665f) is amended by adding at the end the following new subsection:

“(e) GRANTS AND COOPERATIVE AGREEMENTS.—The Director may award financial assistance in the form of grants or cooperative agreements to States, local governments, institutions of higher education (as such term is defined in section 101 of the Higher Education Act of 1965 (20 U.S.C. 1001)), nonprofit organizations, and other non-Federal entities as determined appropriate by the Director for the purpose of funding cybersecurity and infrastructure security education and training programs and initiatives to—

“(1) carry out the purposes of CETAP; and

“(2) enhance CETAP to address the national shortfall of cybersecurity professionals.”.

(b) BRIEFINGS.—Paragraph (2) of subsection (c) of section 2220 of the Homeland Security Act of 2002 (6 U.S.C. 665f) is amended—

(1) by redesignating subparagraphs (C) and (D) as subparagraphs (D) and (E) respectively; and
(2) by inserting after subparagraph (B) the following new subparagraph:

“(C) information on any grants or cooperative agreements made pursuant to subsection (e), including how any such grants or cooperative agreements are being used to enhance cybersecurity education for underserved populations or communities;”.

Subtitle B—Enhancing DHS Acquisitions and Supply Chain

SEC. 59121. HOMELAND PROCUREMENT REFORM.

(a) In general.—Subtitle D of title VIII of the Homeland Security Act of 2002 (6 U.S.C. 391 et seq.) is amended by adding at the end the following new section:

“SEC. 836. REQUIREMENTS TO BUY CERTAIN ITEMS RELATED TO NATIONAL SECURITY INTERESTS.

“(a) Definitions.—In this section:

“(1) Covered item.—The term ‘covered item’ means any of the following:

“(A) Footwear provided as part of a uniform.

“(B) Uniforms.

“(C) Holsters and tactical pouches.

“(D) Patches, insignia, and embellishments.
“(E) Chemical, biological, radiological, and nuclear protective gear.

“(F) Body armor components intended to provide ballistic protection for an individual, consisting of 1 or more of the following:

“(i) Soft ballistic panels.

“(ii) Hard ballistic plates.

“(iii) Concealed armor carriers worn under a uniform.

“(iv) External armor carriers worn over a uniform.

“(G) Any other item of clothing or protective equipment as determined appropriate by the Secretary.

“(2) Frontline Operational Component.—The term ‘frontline operational component’ means any of the following organizations of the Department:

“(A) U.S. Customs and Border Protection.

“(B) U.S. Immigration and Customs Enforcement.

“(C) The United States Secret Service.

“(D) The Transportation Security Administration.

“(E) The Coast Guard.


“(I) The Cybersecurity and Infrastructure Security Agency.

“(b) REQUIREMENTS.—

“(1) IN GENERAL.—The Secretary shall ensure that any procurement of a covered item for a front-line operational component meets the following criteria:

“(A)(i) To the maximum extent possible, not less than one-third of funds obligated in a specific fiscal year for the procurement of such covered items shall be covered items that are manufactured or supplied in the United States by entities that qualify as small business concerns, as such term is described under section 3 of the Small Business Act (15 U.S.C. 632).

“(ii) Covered items may only be supplied pursuant to subparagraph (A) to the extent that United States entities that qualify as small business concerns—
“(I) are unable to manufacture covered items in the United States; and

“(II) meet the criteria identified in subparagraph (B).

“(B) Each contractor with respect to the procurement of such a covered item, including the end-item manufacturer of such a covered item—

“(i) is an entity registered with the System for Award Management (or successor system) administered by the General Services Administration; and

“(ii) is in compliance with ISO 9001:2015 of the International Organization for Standardization (or successor standard) or a standard determined appropriate by the Secretary to ensure the quality of products and adherence to applicable statutory and regulatory requirements.

“(C) Each supplier of such a covered item with an insignia (such as any patch, badge, or emblem) and each supplier of such an insignia, if such covered item with such insignia or such insignia, as the case may be, is not produced,
applied, or assembled in the United States, shall—

“(i) store such covered item with such insignia or such insignia in a locked area;

“(ii) report any pilferage or theft of such covered item with such insignia or such insignia occurring at any stage before delivery of such covered item with such insignia or such insignia; and

“(iii) destroy any such defective or unusable covered item with insignia or insignia in a manner established by the Secretary, and maintain records, for three years after the creation of such records, of such destruction that include the date of such destruction, a description of the covered item with insignia or insignia destroyed, the quantity of the covered item with insignia or insignia destroyed, and the method of destruction.

“(2) WAIVER.—

“(A) IN GENERAL.—In the case of a national emergency declared by the President under the National Emergencies Act (50 U.S.C. 1601 et seq.) or a major disaster declared by
the President under section 401 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5170), the Secretary may waive a requirement in subparagraph (A), (B) or (C) of paragraph (1) if the Secretary determines there is an insufficient supply of a covered item that meets the requirement.

“(B) NOTICE.—Not later than 60 days after the date on which the Secretary determines a waiver under subparagraph (A) is necessary, the Secretary shall provide to the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate and the Committee on Homeland Security, the Committee on Oversight and Reform, and the Committee on Appropriations of the House of Representatives notice of such determination, which shall include—

“(i) identification of the national emergency or major disaster declared by the President;

“(ii) identification of the covered item for which the Secretary intends to issue the waiver; and
“(iii) a description of the demand for
the covered item and corresponding lack of
supply from contractors able to meet the
criteria described in subparagraph (B) or
(C) of paragraph (1).

“(e) PRICING.—The Secretary shall ensure that cov-
ered items are purchased at a fair and reasonable price,
consistent with the procedures and guidelines specified in
the Federal Acquisition Regulation.

“(d) REPORT.—Not later than 1 year after the date
of enactment of this section and annually thereafter, the
Secretary shall provide to the Committee on Homeland Se-
curity, the Committee on Oversight and Reform, and the
Committee on Appropriations of the House of Representa-
tives, and the Committee on Homeland Security and Gov-
ernmental Affairs and the Committee on Appropriations
of the Senate a briefing on instances in which vendors
have failed to meet deadlines for delivery of covered items
and corrective actions taken by the Department in re-
ponse to such instances.

“(e) EFFECTIVE DATE.—This section applies with
respect to a contract entered into by the Department or
any frontline operational component on or after the date
that is 180 days after the date of enactment of this sec-
tion.”.

(b) Study.—

(1) In general.—Not later than 18 months after the date of enactment of this Act, the Secretary of Homeland Security shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a study of the adequacy of uniform allowances provided to employees of frontline operational components (as defined in section 836 of the Homeland Security Act of 2002, as added by subsection (a)).

(2) Requirements.—The study conducted under paragraph (1) shall—

(A) be informed by a Department-wide survey of employees from across the Department of Homeland Security who receive uniform allowances that seeks to ascertain what, if any, improvements could be made to the current uniform allowances and what, if any, impacts current allowances have had on employee morale and retention;

(B) assess the adequacy of the most recent increase made to the uniform allowance for first year employees; and
(C) consider increasing by 50 percent, at minimum, the annual allowance for all other employees.

(c) ADDITIONAL REPORT.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Secretary of Homeland Security shall provide a report with recommendations on how the Department of Homeland Security could procure additional items from domestic sources and bolster the domestic supply chain for items related to national security to—

(A) the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate; and

(B) the Committee on Homeland Security, the Committee on Oversight and Reform, and the Committee on Appropriations of the House of Representatives.

(2) CONTENTS.—The report required under paragraph (1) shall include the following:

(A) A review of the compliance of the Department of Homeland Security with the requirements under section 604 of title VI of division A of the American Recovery and Reinvestment Act of 2009 (6 U.S.C. 453b) to buy cer-
tain items related to national security interests
from sources in the United States.

(B) An assessment of the capacity of the
Department of Homeland Security to procure
the following items from domestic sources:

(i) Personal protective equipment and
other items necessary to respond to a pan-
demic such as that caused by COVID–19.

(ii) Helmets that provide ballistic pro-
tection and other head protection and com-
ponents.

(iii) Rain gear, cold weather gear, and
other environmental and flame resistant
clothing.

(d) CLERICAL AMENDMENT.—The table of contents
in section 1(b) of the Homeland Security Act of 2002
(Public Law 107–296; 116 Stat. 2135) is amended by in-
serting after the item relating to section 835 the following:

"Sec. 836. Requirements to buy certain items related to national security inter-
ests.”.

SEC. 59122. DHS SOFTWARE SUPPLY CHAIN RISK MANAGE-
MENT.

(a) GUIDANCE.—The Secretary of Homeland Secu-
rity, acting through the Under Secretary, shall issue guid-
ance with respect to new and existing covered contracts.
(b) NEW COVERED CONTRACTS.—In developing guidance under subsection (a), with respect to each new covered contract, as a condition on the award of such a contract, each contractor responding to a solicitation for such a contract shall submit to the covered officer—

(1) a planned bill of materials when submitting a bid proposal; and

(2) the certification and notifications described in subsection (e).

(c) EXISTING COVERED CONTRACTS.—In developing guidance under subsection (a), with respect to each existing covered contract, each contractor with an existing covered contract shall submit to the covered officer—

(1) the bill of materials used for such contract, upon the request of such officer; and

(2) the certification and notifications described in subsection (e).

(d) UPDATING BILL OF MATERIALS.—With respect to a covered contract, in the case of a change to the information included in a bill of materials submitted pursuant to subsections (b)(1) and (c)(1), each contractor shall submit to the covered officer the update to such bill of materials, in a timely manner.

(e) CERTIFICATION AND NOTIFICATIONS.—The certification and notifications referred to in subsections
(b)(2) and (c)(2), with respect to a covered contract, are
the following:

1. A certification that each item listed on the
submitted bill of materials is free from all known
vulnerabilities or defects affecting the security of the
end product or service identified in—

   (A) the National Institute of Standards
and Technology National Vulnerability Data-
base; and

   (B) any database designated by the Under
Secretary, in coordination with the Director of
the Cybersecurity and Infrastructure Security
Agency, that tracks security vulnerabilities and
defects in open source or third-party developed
software.

2. A notification of each vulnerability or defect
affecting the security of the end product or service,
if identified, through—

   (A) the certification of such submitted bill
of materials required under paragraph (1); or

   (B) any other manner of identification.

3. A notification relating to the plan to miti-
gate, repair, or resolve each security vulnerability or
defect listed in the notification required under para-
graph (2).
(f) Enforcement.—In developing guidance under subsection (a), the Secretary shall instruct covered officers with respect to—

(1) the processes available to such officers enforcing subsections (b) and (c); and

(2) when such processes should be used.

(g) Effective Date.—The guidance required under subsection (a) shall take effect on the date that is 180 days after the date of the enactment of this section.

(h) GAO Report.—Not later than 1 year after the date of the enactment of this Act, the Comptroller General of the United States shall submit to the Secretary, the Committee on Homeland Security of the House of Representatives, and the Committee on Homeland Security and Governmental Affairs of the Senate a report that includes—

(1) a review of the implementation of this section;

(2) information relating to the engagement of the Department of Homeland Security with industry;

(3) an assessment of how the guidance issued pursuant to subsection (a) complies with Executive Order 14208 (86 Fed. Reg. 26633; relating to improving the nation’s cybersecurity); and
(4) any recommendations relating to improving the supply chain with respect to covered contracts.

(i) DEFINITIONS.—In this section:

(1) BILL OF MATERIALS.—The term “bill of materials” means a list of the parts and components (whether new or reused) of an end product or service, including, with respect to each part and component, information relating to the origin, composition, integrity, and any other information as determined appropriate by the Under Secretary.

(2) COVERED CONTRACT.—The term “covered contract” means a contract relating to the procurement of covered information and communications technology or services for the Department of Homeland Security.

(3) COVERED INFORMATION AND COMMUNICATIONS TECHNOLOGY OR SERVICES.—The term “covered information and communications technology or services” means the terms—

(A) “information technology” (as such term is defined in section 11101(6) of title 40, United States Code);

(B) “information system” (as such term is defined in section 3502(8) of title 44, United States Code);
(C) “telecommunications equipment” (as such term is defined in section 3(52) of the Communications Act of 1934 (47 U.S.C. 153(52))); and

(D) “telecommunications service” (as such term is defined in section 3(53) of the Communications Act of 1934 (47 U.S.C. 153(53))).

(4) COVERED OFFICER.—The term “covered officer” means—

(A) a contracting officer of the Department; and

(B) any other official of the Department as determined appropriate by the Under Secretary.

(5) SOFTWARE.—The term “software” means computer programs and associated data that may be dynamically written or modified during execution.

(6) UNDER SECRETARY.—The term “Under Secretary” means the Under Secretary for Management of the Department of Homeland Security.

SEC. 59123. DEPARTMENT OF HOMELAND SECURITY MENTOR-PROTÉGÉ PROGRAM.

(a) IN GENERAL.—Subtitle H of title VIII of the Homeland Security Act of 2002 (6 U.S.C. 451 et seq.) is amended by adding at the end the following new section:
“SEC. 890C. MENTOR-PROTÉGÉ PROGRAM.

“(a) Establishment.—There is established in the Department a mentor-protégé program (in this section referred to as the ‘Program’) under which a mentor firm enters into an agreement with a protégé firm for the purpose of assisting the protégé firm to compete for prime contracts and subcontracts of the Department.

“(b) Eligibility.—The Secretary shall establish criteria for mentor firms and protégé firms to be eligible to participate in the Program, including a requirement that a firm is not included on any list maintained by the Federal Government of contractors that have been suspended or debarred.

“(c) Program Application and Approval.—

“(1) Application.—The Secretary, acting through the Office of Small and Disadvantaged Business Utilization of the Department, shall establish a process for submission of an application jointly by a mentor firm and the protégé firm selected by the mentor firm. The application shall include each of the following:

“(A) A description of the assistance to be provided by the mentor firm, including, to the extent available, the number and a brief description of each anticipated subcontract to be awarded to the protégé firm.
“(B) A schedule with milestones for achieving the assistance to be provided over the period of participation in the Program.

“(C) An estimate of the costs to be incurred by the mentor firm for providing assistance under the Program.

“(D) Attestations that Program participants will submit to the Secretary reports at times specified by the Secretary to assist the Secretary in evaluating the protégé firm’s developmental progress.

“(E) Attestations that Program participants will inform the Secretary in the event of a change in eligibility or voluntary withdrawal from the Program.

“(2) APPROVAL.—Not later than 60 days after receipt of an application pursuant to paragraph (1), the head of the Office of Small and Disadvantaged Business Utilization shall notify applicants of approval or, in the case of disapproval, the process for resubmitting an application for reconsideration.

“(3) RESCISSION.—The head of the Office of Small and Disadvantaged Business Utilization may rescind the approval of an application under this
subsection if it determines that such action is in the
best interest of the Department.

“(d) Program Duration.—A mentor firm and
protégé firm approved under subsection (c) shall enter into
an agreement to participate in the Program for a period
of not less than 36 months.

“(e) Program Benefits.—A mentor firm and
protégé firm that enter into an agreement under sub-
section (d) may receive the following Program benefits:

“(1) With respect to an award of a contract
that requires a subcontracting plan, a mentor firm
may receive evaluation credit for participating in the
Program.

“(2) With respect to an award of a contract
that requires a subcontracting plan, a mentor firm
may receive credit for a protégé firm performing as
a first tier subcontractor or a subcontractor at any
tier in an amount equal to the total dollar value of
any subcontracts awarded to such protégé firm.

“(3) A protégé firm may receive technical, man-
gerinal, financial, or any other mutually agreed upon
benefit from a mentor firm, including a subcontract
award.

“(f) Reporting.—Not later than one year after the
date of the enactment of this Act, and annually thereafter,
the head of the Office of Small and Disadvantaged Business Utilization shall submit to the Committee on Homeland Security and Governmental Affairs and the Committee on Small Business and Entrepreneurship of the Senate and the Committee on Homeland Security and the Committee on Small Business of the House of Representatives a report that—

“(1) identifies each agreement between a mentor firm and a protégé firm entered into under this section, including the number of protégé firm participants that are—

“(A) small business concerns;

“(B) small business concerns owned and controlled by veterans;

“(C) small business concerns owned and controlled by service-disabled veterans;

“(D) qualified HUBZone small business concerns;

“(E) small business concerns owned and controlled by socially and economically disadvantaged individuals;

“(F) small business concerns owned and controlled by women;

“(G) historically Black colleges and universities; and
“(H) minority-serving institutions;

“(2) describes the type of assistance provided
by mentor firms to protégé firms;

“(3) identifies contracts within the Department
in which a mentor firm serving as the prime con-
tractor provided subcontracts to a protégé firm
under the Program; and

“(4) assesses the degree to which there has
been—

“(A) an increase in the technical capabili-
ties of protégé firms; and

“(B) an increase in the quantity and esti-
imated value of prime contract and subcontract
awards to protégé firms for the period covered
by the report.

“(g) RULE OF CONSTRUCTION.—Nothing in this sec-
tion may be construed to limit, diminish, impair, or other-
wise affect the authority of the Department to participate
in any program carried out by or requiring approval of
the Small Business Administration or adopt or follow any
regulation or policy that the Administrator of the Small
Business Administration may promulgate, except that, to
the extent that any provision of this section (including
subsection (h)) conflicts with any other provision of law,
regulation, or policy, this section shall control.
“(h) 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 of the Higher Education Act of 1965 (20 U.S.C. 1061).

“(2) MENTOR FIRM.—The term ‘mentor firm’ means a for-profit business concern that is not a small business concern that—

“(A) has the ability to assist and commits to assisting a protégé to compete for Federal prime contracts and subcontracts; and

“(B) satisfies any other requirements imposed by the Secretary.

“(3) MINORITY-SERVING INSTITUTION.—The term ‘minority-serving institution’ means an institution of higher education described in section 317 of the Higher Education Act of 1965 (20 U.S.C. 1067q(a)).

“(4) PROTÉGÉ FIRM.—The term ‘protégé firm’ means a small business concern, a historically Black college or university, or a minority-serving institution that—

“(A) is eligible to enter into a prime contract or subcontract with the Department; and
“(B) satisfies any other requirements imposed by the Secretary.

“(5) SMALL BUSINESS ACT DEFINITIONS.—The terms ‘small business concern’, ‘small business concern owned and controlled by veterans’, ‘small business concern owned and controlled by service-disabled veterans’, ‘qualified HUBZone small business concern’, ‘and small business concern owned and controlled by women’ have the meanings given such terms, respectively, under section 3 of the Small Business Act (15 U.S.C. 632). The term ‘small business concern owned and controlled by socially and economically disadvantaged individuals’ has the meaning given such term in section 8(d)(3)(C) of the Small Business Act (15 U.S.C. 637(d)(3)(C)).”.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 890B the following new item:

“Sec. 890C. Mentor-protégé program.”.

SEC. 59124. DHS TRADE AND ECONOMIC SECURITY COUNCIL.

(a) DHS TRADE AND ECONOMIC SECURITY COUNCIL.—

et seq.) is further amended by adding at the end the following new section:

“SEC. 890D. DHS TRADE AND ECONOMIC SECURITY COUNCIL.

“(a) ESTABLISHMENT.—There is established in the Department the DHS Trade and Economic Security Council (referred to in this section as the ‘Council’).

“(b) DUTIES OF THE COUNCIL.—The Council shall provide to the Secretary advice and recommendations on matters of trade and economic security, including—

“(1) identifying concentrated risks for trade and economic security;

“(2) setting priorities for securing the Nation’s trade and economic security;

“(3) coordinating Department-wide activity on trade and economic security matters;

“(4) with respect to the President’s continuity of the economy plan under section 9603 of the William M. (Mac) Thornberry National Defense Authorization Act of Fiscal Year 2021;

“(5) proposing statutory and regulatory changes impacting trade and economic security; and

“(6) any other matters the Secretary considers appropriate.

“(c) MEMBERSHIP.—
“(1) IN GENERAL.—The Council shall be composed of the following members:


“(B) An officer or an employee, selected by the Secretary, from each of the following components and offices of the Department:

“(i) The Cybersecurity and Infrastructure Security Agency.


“(iii) The Office of Intelligence and Analysis.

“(iv) The Science and Technology Directorate.


“(vi) The Coast Guard.

“(vii) U.S. Customs and Border Protection.

“(viii) U.S. Immigration and Customs Enforcement.

“(ix) The Transportation Security Administration.
“(2) CHAIR AND VICE CHAIR.—The Assistant Secretary for Trade and Economic Security shall serve as Chair of the Council. The Assistant Secretary for Trade and Economic Security may designate a Council member as a Vice Chair.

“(d) MEETINGS.—The Council shall meet not less frequently than quarterly, as well as—

“(1) at the call of the Chair; or

“(2) at the direction of the Secretary.

“(e) BRIEFINGS.—Not later than 180 days after the date of the enactment of this section and every six months thereafter for four years, the Council shall brief the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate on the actions and activities of the Council.

“(f) DEFINITION.—In this section, the term ‘economic security’ means the condition of having secure and resilient domestic production capacity combined with reliable access to the global resources necessary to maintain an acceptable standard of living and protect core national values.”.

(2) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act
of 2002 is amended by inserting after the item relating to section 890C the following new item:

“Sec. 890D. DHS Trade and Economic Security Council.”.

(b) ASSISTANT SECRETARY FOR TRADE AND ECONOMIC SECURITY.—Section 709 of the Homeland Security Act of 2002 (6 U.S.C. 349) is amended—

(1) by redesignating subsection (g) as subsection (h); and

(2) by inserting after subsection (f) the following new subsection:

“(g) ASSISTANT SECRETARY FOR TRADE AND ECONOMIC SECURITY.—

“(1) IN GENERAL.—There is within the Office of Strategy, Policy, and Plans an Assistant Secretary for Trade and Economic Security.

“(2) DUTIES.—The Assistant Secretary for Trade and Economic Security shall be responsible for policy formulation regarding matters relating to economic security and trade, as such matters relate to the mission and the operations of the Department.

“(3) ADDITIONAL RESPONSIBILITIES.—In addition to the duties specified in paragraph (2), the Assistant Secretary for Trade and Economic Security shall—

“(A) oversee—
“(i) the activities and enhancements of requirements for supply chain mapping not otherwise assigned by law or by the Secretary to another officer; and

“(ii) assessments and reports to Congress related to critical economic security domains;

“(B) serve as the executive for the Department on the Committee on Foreign Investment in the United States (CFIUS), the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector, and the Federal Acquisition Security Council (in addition to any position on such Council occupied by a representative of the Cybersecurity and Infrastructure Security Agency of the Department);

“(C) coordinate with stakeholders in other Federal departments and agencies and non-governmental entities with trade and economic security interests, authorities, and responsibilities; and

“(D) perform such additional duties as the Secretary or the Under Secretary of Strategy, Policy, and Plans may prescribe.
“(4) DEFINITIONS.—In this subsection:

“(A) CRITICAL ECONOMIC SECURITY DOMAIN.—The term ‘critical economic security domain’ means any infrastructure, industry, technology, or intellectual property (or combination thereof) that is essential for the economic security of the United States.

“(B) ECONOMIC SECURITY.—The term ‘economic security’ has the meaning given such term in section 890B.”.

(c) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Secretary of Homeland Security $3,000,000 for each of fiscal years 2023 through 2027 to carry out section 890B and subsection (g) of section 709 of the Homeland Security Act of 2002, as added and inserted, respectively, by subsections (a) and (b) of this Act.

SEC. 59125. DHS ACQUISITION REFORM.


(1) in subsection (a)—
(A) in paragraph (2), by inserting “and acquisition management” after “Procurement”; and

(B) in paragraph (6), by inserting “(including firearms and other sensitive assets)” after “equipment”;

(2) by redesignating subsections (d), the first subsection (e) (relating to the system for award management consultation), and the second subsection (e) (relating to the definition of interoperable communications) as subsections (e), (f), and (g), respectively; and

(3) by inserting after subsection (c) the following new subsection:

“(d) ACQUISITION AND RELATED RESPONSIBILITIES.—

“(1) IN GENERAL.—Notwithstanding section 1702(a) of title 41, United States Code, the Under Secretary for Management is the Chief Acquisition Officer of the Department. As Chief Acquisition Officer, the Under Secretary shall have the authorities and perform the functions specified in section 1702(b) of such title, and perform all other functions and responsibilities delegated by the Secretary or described in this subsection.
“(2) FUNCTIONS AND RESPONSIBILITIES.—In addition to the authorities and functions specified in section 1702(b) of title 41, United States Code, the functions and responsibilities of the Under Secretary for Management related to acquisition (as such term is defined in section 131 of such title) include the following:

“(A) Advising the Secretary regarding acquisition management activities, considering risks of failure to achieve cost, schedule, or performance parameters, to ensure that the Department achieves its mission through the adoption of widely accepted program management best practices (as such term is defined in section 837) and standards and, where appropriate, acquisition innovation best practices.

“(B) Leading the Department’s acquisition oversight body, the Acquisition Review Board.

“(C) Synchronizing interagency coordination relating to acquisition programs and acquisition management efforts of the Department.

“(D) Exercising the acquisition decision authority (as such term is defined in section 837) to approve, pause, modify (including the rescission of approvals of program milestones),
or cancel major acquisition programs (as such term is defined in section 837), unless the Under Secretary delegates such authority to a Component Acquisition Executive (as such term is defined in section 837) pursuant to paragraph (3).

“(E) Providing additional scrutiny and oversight for an acquisition that is not a major acquisition if—

“(i) the acquisition is for a program that is important to the strategic and performance plans of the Department;

“(ii) the acquisition is for a program with significant program or policy implications; and

“(iii) the Secretary determines that such scrutiny and oversight for the acquisition is proper and necessary.

“(F) Establishing policies for managing acquisitions across the Department that promote best practices (as such term is defined in section 837).

“(G) Establishing policies for acquisition that implement an approach that considers risks of failure to achieve cost, schedule, or per-
formance parameters that all components of the Department shall comply with, including outlining relevant authorities for program managers to effectively manage acquisition programs (as such term is defined in section 837).

“(H) Ensuring that each major acquisition program has a Department-approved acquisition program baseline (as such term is defined in section 837), pursuant to the Department’s acquisition management policy that is traceable to the life-cycle cost estimate of the program, integrated master schedule, and operational requirements.

“(I) Assisting the heads of components and Component Acquisition Executives in efforts to comply with Federal law, the Federal Acquisition Regulation, and Department acquisition management directives.

“(J) Ensuring that grants and financial assistance are provided only to individuals and organizations that are not suspended or debarred.

“(K) Distributing guidance throughout the Department to ensure that contractors involved in acquisitions, particularly contractors that ac-
cess the Department’s information systems and technologies, adhere to relevant Department policies related to physical and information security as identified by the Under Secretary.

“(L) Overseeing the Component Acquisition Executive organizational structure to ensure Component Acquisition Executives have sufficient capabilities and comply with Department acquisition policies.

“(M) Developing and managing a professional acquisition workforce to ensure the goods and services acquired by the Department meet the needs of the mission and are at the best value for the expenditure of public resources.

“(3) DELEGATION OF CERTAIN ACQUISITION DECISION AUTHORITY.—The Under Secretary for Management may delegate acquisition decision authority, in writing, to the relevant Component Acquisition Executive for a major capital asset, service, or hybrid acquisition program that has a life-cycle cost estimate of at least $300,000,000 but not more than $1,000,000,000, based on fiscal year 2022 constant dollars, if—

“(A) the component concerned possesses working policies, processes, and procedures that
are consistent with Department acquisition policy;

“(B) the Component Acquisition Executive concerned has adequate, experienced, and dedicated professional employees with program management training; and

“(C) each major acquisition program has a Department-approved acquisition program baseline, and it is meeting agreed-upon cost, schedule, and performance thresholds.”.

(b) Office of Test and Evaluation of the Department of Homeland Security.—

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

“SEC. 323. OFFICE OF TEST AND EVALUATION.

“(a) Establishment of Office.—There is established in the Directorate of Science and Technology of the Department an Office of Test and Evaluation (in this section referred to as the ‘Office’). The Office shall—

“(1) serve as the principal advisory office for test and evaluation support across the Department; and
“(2) serve as the test and evaluation liaison

with—

“(A) Federal agencies and foreign, State, local, Tribal, and territorial governments;

“(B) the private sector;

“(C) institutions of higher education; and

“(D) other relevant entities.

“(b) DIRECTOR.—The Office shall be led by a Director. The Director shall oversee the duties specified in subsection (a) and carry out the following responsibilities:

“(1) Serve as a member of the Department’s Acquisition Review Board.

“(2) Establish and update, as necessary, test and evaluation policies, procedures, and guidance for the Department.

“(3) Ensure, in coordination with the Chief Acquisition Officer, the Joint Requirements Council, the Under Secretary for Science and Technology, and relevant component heads, that acquisition programs (as such term is defined in section 837)—

“(A) complete reviews of operational requirements to ensure such requirements—

“(i) are informed by threats, including physical and cybersecurity threats;

“(ii) are operationally relevant; and
“(iii) are measurable, testable, and achievable within the constraints of cost and schedule;

“(B) complete independent testing and evaluation of a system or service throughout development of such system or service;

“(C) complete operational testing and evaluation that includes all system components and incorporates operators into such testing and evaluation to ensure that a system or service satisfies the mission requirements in the operational environment of such system or service as intended in the acquisition program baseline;

“(D) use independent verification and validation of test and evaluation implementation and results, as appropriate; and

“(E) document whether such programs meet all operational requirements.

“(4) Provide oversight of test and evaluation activities for major acquisition programs throughout the acquisition life cycle by—

“(A) approving program test and evaluation master plans, plans for individual test and evaluation events, and other related documentation, determined appropriate by the Director;
“(B) approving which independent test and evaluation agent or third-party tester is selected for each program; and

“(C) providing an independent assessment to the acquisition decision authority (as such term is defined in section 837) that assesses a program’s progress in meeting operational requirements and operational effectiveness, suitability, and resilience to inform production and deployment decisions.

“(5) Determine if testing of a system or service conducted by other Federal agencies, entities, or institutions of higher education are relevant and sufficient in determining whether such system or service performs as intended.

“(e) ANNUAL REPORT.—

“(1) IN GENERAL.—Not later than one year after the date of the enactment of this section and annually thereafter, the Director of the Office shall submit to the Secretary, the Under Secretary for Management, component heads, and the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs a report relating to the test and evaluation activities of the major acquisition
programs of the Department for the previous fiscal year.

“(2) ELEMENTS.—Each report required under paragraph (1) shall include the following:

“(A) An assessment of—

“(i) test and evaluation activities conducted for each major acquisition program with respect to demonstrating operational requirements and operational effectiveness, suitability, and resilience for each such program;

“(ii) any waivers of, or deviations from, approved program test and evaluation master plans referred to in subsection (b)(3)(A);

“(iii) any concerns raised by the independent test and evaluation agent or third-party tester selected and approved under subsection (b)(3)(B) relating to such waivers or deviations; and

“(iv) any actions that have been taken or are planned to be taken to address such concerns.

“(B) Recommendations with respect to resources, facilities, and levels of funding made
available for test and evaluation activities referred to in subparagraph (A).

“(3) FORM.—Each report required under paragraph (1) shall be submitted in unclassified form but may include a classified annex.

“(d) RELATIONSHIP TO UNDER SECRETARY FOR SCIENCE AND TECHNOLOGY.—

“(1) IN GENERAL.—The Under Secretary for Management and the Under Secretary for Science and Technology shall coordinate in matters related to Department-wide acquisitions so that investments of the Directorate of Science and Technology are able to support current and future requirements of the components of the Department.

“(2) RULE OF CONSTRUCTION.—Nothing in this subsection may be construed as affecting or diminishing the authority of the Under Secretary for Science and Technology.”.

(2) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 322 the following new item:

“Sec. 323. Office of Test and Evaluation.”.

(e) ACQUISITION AUTHORITIES FOR CHIEF FINANCIAL OFFICER OF THE DEPARTMENT OF HOMELAND SECURITY.—Paragraph (2) of section 702(b) of the Home-
land Security Act of 2002 (6 U.S.C. 342(b)) is amended by—

(1) redesignating subparagraph (I) as subparagraph (J); and

(2) inserting after subparagraph (H) the following new subparagraph:

“(I) Oversee the costs of acquisition programs (as such term is defined in section 837) and related activities to ensure that actual and planned costs are in accordance with budget estimates and are affordable, or can be adequately funded, over the life cycle of such programs and activities.”.

(d) ACQUISITION AUTHORITIES FOR CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF HOMELAND SECURITY.—Section 703 of the Homeland Security Act of 2002 (6 U.S.C. 343) is amended—

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

(2) by inserting after subsection (a) the following new subsection:

“(b) ACQUISITION RESPONSIBILITIES.—In addition to the responsibilities specified in section 11315 of title 40, United States Code, the acquisition responsibilities of the Chief Information Officer, in consultation with the
Under Secretary for Management, shall include the following:

“(1) Overseeing the management of the Homeland Security Enterprise Architecture and ensuring that, before each acquisition decision event (as such term is defined in section 837), approved information technology acquisitions comply with any departmental information technology management requirements, security protocols, and the Homeland Security Enterprise Architecture, and in any case in which information technology acquisitions do not so comply, making recommendations to the Department’s Acquisition Review Board regarding such noncompliance.

“(2) Providing recommendations to the Acquisition Review Board regarding information technology programs and developing information technology acquisition strategic guidance.”.

(c) Acquisition Authorities for Under Secretary of Strategy, Policy, and Plans of the Department of Homeland Security.—Subsection (c) of section 709 of the Homeland Security Act of 2002 (6 U.S.C. 349) is amended by—

(1) redesignating paragraphs (4) through (7) as (5) through (8), respectively; and
(2) inserting after paragraph (3) the following new paragraph:

“(4) ensure acquisition programs (as such term is defined in section 837) support the DHS Quadrennial Homeland Security Review Report, the DHS Strategic Plan, the DHS Strategic Priorities, and other appropriate successor documents;”.

(f) Acquisition Authorities for Program Accountability and Risk Management (PARM) of the Department of Homeland Security.—

(1) In general.—Title VII of the Homeland Security Act of 2002 (6 U.S.C. 341 et seq.), as amended by this Act, is further amended by adding at the end the following new section:

“SEC. 715. PROGRAM ACCOUNTABILITY AND RISK MANAGEMENT OFFICE.

“(a) Establishment of Office.—There is established in the Management Directorate of the Department a Program Accountability and Risk Management office. Such office shall—

“(1) provide consistent accountability, standardization, and transparency of major acquisition programs of the Department;

“(2) serve as the central oversight function for all Department major acquisition programs; and
“(3) provide review and analysis of Department acquisition programs, as appropriate.

“(b) EXECUTIVE DIRECTOR.—The Program Accountability and Risk Management office shall be led by an Executive Director. The Executive Director shall oversee the duties specified in subsection (a), report directly to the Under Secretary for Management, and carry out the following responsibilities:

“(1) Regularly monitor the performance of Department major acquisition programs between acquisition decision events to identify problems with cost, performance, or schedule that components may need to address to prevent cost overruns, performance issues, or schedule delays.

“(2) Assist the Under Secretary for Management in managing the Department’s acquisition programs, acquisition workforce, and related activities of the Department.

“(3) Conduct oversight of individual acquisition programs to implement Department acquisition program policy, procedures, and guidance, with a priority on ensuring the data the office collects and maintains from Department components is accurate and reliable.
“(4) Serve as the focal point and coordinator for the acquisition life-cycle review process and as the executive secretariat for the Department’s Acquisition Review Board.

“(5) Advise the persons having acquisition decision authority to—

“(A) make acquisition decisions consistent with all applicable laws; and

“(B) establish clear lines of authority, accountability, and responsibility for acquisition decision-making within the Department.

“(6) Develop standardized certification standards, in consultation with the Component Acquisition Executives, for all acquisition program managers.

“(7) Assess the results of major acquisition programs’ post-implementation reviews, and identify opportunities to improve performance throughout the acquisition process.

“(8) Provide technical support and assistance to Department acquisition programs and acquisition personnel, and coordinate with the Chief Procurement Officer regarding workforce training and development activities.
“(9) Assist, as appropriate, with the preparation of the Future Years Homeland Security Program, and make such information available to the congressional homeland security committees.

“(10) In coordination with the Component Acquisition Executives, maintain the Master Acquisition Oversight List, updated quarterly, that shall serve as an inventory of all major acquisition programs and non-major acquisition programs within the Department, including for each such program—

“(A) the component sponsoring the acquisition;

“(B) the name of the acquisition;

“(C) the acquisition level as determined by the anticipated life-cycle cost of the program and other criteria pursuant to the Department-level acquisition policy;

“(D) the acquisition decision authority for the acquisition; and

“(E) the current acquisition phase.

“(c) RESPONSIBILITIES OF COMPONENTS.—Each head of a component shall comply with Federal law, the Federal Acquisition Regulation, and Department acquisition management directives established by the Under Sec-
For each major acquisition program, each head of a component shall—

“(1) establish an organizational structure for conducting acquisitions within the component, to be managed by a Component Acquisition Executive;

“(2) obtain the resources necessary to operate such an organizational structure that are aligned with the number, type, size, and complexity of the acquisition programs of the component; and

“(3) oversee sustainment of capabilities deployed by major acquisition programs and non-major acquisition programs after all planned deployments are completed until such capabilities are retired or replaced.

“(d) RESPONSIBILITIES OF COMPONENT ACQUISITION EXECUTIVES.—Each Component Acquisition Executive shall—

“(1) establish and implement policies and guidance for managing and conducting oversight for major acquisition programs and non-major acquisition programs within the component at issue that comply with Federal law, the Federal Acquisition Regulation, and Department acquisition management directives established by the Under Secretary for Management;
“(2) for each major acquisition program—

“(A) define baseline requirements and document changes to such requirements, as appropriate;

“(B) establish a complete life cycle cost estimate with supporting documentation that is consistent with cost estimating best practices as identified by the Comptroller General of the United States;

“(C) verify each life cycle cost estimate against independent cost estimates or assessments, as appropriate, and reconcile any differences;

“(D) complete a cost-benefit analysis with supporting documentation; and

“(E) develop and maintain a schedule that is consistent with scheduling best practices as identified by the Comptroller General of the United States, including, in appropriate cases, an integrated master schedule;

“(3) ensure that all acquisition program documentation provided by the component demonstrates the knowledge required for successful program execution prior to final approval and is complete, accurate, timely, and valid;
“(4) in such cases where it is appropriate, exercise the acquisition decision authority to approve, pause, modify (including the rescission of approvals of program milestones), or cancel major acquisition programs or non-major acquisition programs when delegated by the Under Secretary for Management pursuant to section 701(d)(3); and

“(5) review, oversee, and direct activities between acquisition decision events for major acquisition programs within the component for which the Under Secretary for Management is the acquisition decision authority.

“(e) DEFINITIONS.—In this section:

“(1) ACQUISITION.—The term ‘acquisition’ has the meaning given such term in section 131 of title 41, United States Code.

“(2) ACQUISITION DECISION AUTHORITY.—The term ‘acquisition decision authority’ means the authority, in addition to the authorities and functions specified in subsection (b) of section 1702 of title 41, United States Code, held by the Secretary acting through the Under Secretary for Management to—

“(A) ensure compliance with Federal law, the Federal Acquisition Regulation, and Department acquisition management directives;
“(B) review (including approving, pausing, modifying, or canceling) an acquisition program throughout the life cycle of such program;

“(C) ensure that acquisition program managers have the resources necessary to successfully execute an approved acquisition program;

“(D) ensure appropriate acquisition program management of cost, schedule, risk, and system or service performance of the acquisition program at issue, including assessing acquisition program baseline breaches and directing any corrective action for such breaches;

“(E) ensure that acquisition program managers, on an ongoing basis, monitor cost, schedule, and performance against established baselines and use tools to assess risks to an acquisition program at all phases of the life-cycle of such program; and

“(F) establish policies and procedures for major acquisition programs of the Department.

“(3) ACQUISITION DECISION EVENT.—The term ‘acquisition decision event’, with respect to an acquisition program, means a predetermined point within the acquisition life-cycle at which the acquisition de-
cision authority determines whether such acquisition program shall proceed to the next acquisition phase.

“(4) ACQUISITION PROGRAM.—The term ‘acquisition program’ means the conceptualization, initiation, design, development, test, contracting, production, deployment, logistics support, modification, or disposal of systems, supplies, or services (including construction) to satisfy the Department’s needs.

“(5) ACQUISITION PROGRAM BASELINE.—The term ‘acquisition program baseline’, with respect to an acquisition program, means the cost, schedule, and performance parameters, expressed in standard, measurable, quantitative terms, which must be met to accomplish the goals of such program.

“(6) BEST PRACTICES.—The term ‘best practices’, with respect to acquisition, means a knowledge-based approach to capability development, procurement, and support that includes the following:

“(A) Identifying and validating needs.

“(B) Assessing alternatives to select the most appropriate solution.

“(C) Establishing well-defined requirements.
“(D) Developing realistic cost assessments and schedules that account for the entire life-cycle of an acquisition.

“(E) Demonstrating technology, design, and manufacturing maturity before initiating production.

“(F) Using milestones and exit criteria or specific accomplishments that demonstrate the attainment of knowledge to support progress throughout the acquisition phases.

“(G) Regularly assessing and managing risks to achieve requirements and cost and schedule goals.

“(H) To the maximum extent possible, adopting and executing standardized processes.

“(I) Establishing a workforce that is qualified to perform necessary acquisition roles.

“(J) Integrating into the Department’s mission and business operations the capabilities described in subparagraphs (A) through (I).

“(7) BREACH.—The term ‘breach’, with respect to a major acquisition program, means a failure to meet any cost, schedule, or performance threshold specified in the most recently approved acquisition program baseline.
“(8) CONGRESSIONAL HOMELAND SECURITY COMMITTEES.—The term ‘congressional homeland security committees’ means—

“(A) the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate; and

“(B) the Committee on Appropriations of the House of Representatives and the Committee on Appropriations of the Senate.

“(9) COMPONENT ACQUISITION EXECUTIVE.—
The term ‘Component Acquisition Executive’ means the senior acquisition official within a component who is designated in writing by the Under Secretary for Management, in consultation with the component head, with authority and responsibility for leading a process and staff to provide acquisition and program management oversight, policy, and guidance to ensure that statutory, regulatory, and higher level policy requirements are fulfilled, including compliance with Federal law, the Federal Acquisition Regulation, and Department acquisition management directives established by the Under Secretary.

“(10) LIFE-CYCLE COST.—The term ‘life-cycle cost’ means the total cost to the Government of ac-
quiring, operating, supporting, and (if applicable) disposing of the items being acquired.

“(11) MAJOR ACQUISITION PROGRAM.—The term ‘major acquisition program’ means a Department capital asset, services, or hybrid acquisition program that is estimated by the Secretary to require an eventual total expenditure of at least $300,000,000 (based on fiscal year 2022 constant dollars) over its life cycle or a program identified by the Chief Acquisition Officer as a program of special interest.”.

(2) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 714 the following new item:

“Sec. 715. Program Accountability and Risk Management office.”.

(g) ACQUISITION DOCUMENTATION.—

(1) IN GENERAL.—Subtitle D of title VIII of the Homeland Security Act of 2002 (6 U.S.C. 391 et seq.), as amended by this Act, is further amended by adding at the end the following new section:

“SEC. 837. ACQUISITION DOCUMENTATION.

“For each major acquisition program (as such term is defined in section 714), the Secretary, acting through the Under Secretary for Management, shall require the
head of each relevant component or office of the Department to—

“(1) maintain acquisition documentation that is complete, accurate, timely, and valid, and that includes—

“(A) operational requirements that are validated consistent with departmental policy;

“(B) a complete life-cycle cost estimate with supporting documentation;

“(C) verification of such life-cycle cost estimate against independent cost estimates, and reconciliation of any differences;

“(D) a cost-benefit analysis with supporting documentation;

“(E) an integrated master schedule with supporting documentation;

“(F) plans for conducting systems engineering reviews and test and evaluation activities throughout development to support production and deployment decisions;

“(G) an acquisition plan that outlines the procurement approach, including planned contracting vehicles;

“(H) a logistics and support plan for operating and maintaining deployed capabilities
until such capabilities are disposed of or retired;

and

“(I) an acquisition program baseline that is traceable to the operational requirements of the program required under subparagraphs (A), (B), and (E);

“(2) prepare cost estimates and schedules for major acquisition programs pursuant to subparagraphs (B) and (E) of paragraph (1) in a manner consistent with best practices as identified by the Comptroller General of the United States; and

“(3) ensure any revisions to the acquisition documentation maintained pursuant to paragraph (1) are reviewed and approved in accordance with departmental policy.”.

(2) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by adding after the item relating to section 836 the following new item:

“Sec. 837. Acquisition documentation.”.

SEC. 59126. DHS ACQUISITION REVIEW BOARD.

(a) IN GENERAL.—Subtitle D of title VIII of the Homeland Security Act of 2002 (6 U.S.C. 391 et seq.) is further amended by adding at the end the following new section:
"SEC. 838. ACQUISITION REVIEW BOARD.

(a) IN GENERAL.—There is established in the Department an Acquisition Review Board (in this section referred to as the ‘Board’) to support the Under Secretary for Management in managing the Department’s acquisitions.

(b) COMPOSITION.—

(1) CHAIR.—The Under Secretary for Management shall serve as chair of the Board.

(2) OVERSIGHT.—The Under Secretary for Management may designate an employee of the Department to oversee the operations of the Board.

(3) PARTICIPATION.—The Under Secretary for Management shall ensure participation by other relevant Department officials with responsibilities related to acquisitions as permanent members of the Board, including the following:

(A) The Chair of the Joint Requirements Council.

(B) The Chief Financial Officer.

(C) The Chief Human Capital Officer.

(D) The Chief Information Officer.

(E) The Chief Procurement Officer.

(F) The Chief Readiness Support Officer.

(G) The Chief Security Officer.
“(H) The Director of the Office of Test and Evaluation.

“(I) Other relevant senior Department officials, as designated by the Under Secretary for Management.

“(c) MEETINGS.—The Board shall meet regularly for purposes of evaluating the progress and status of an acquisition program. The Board shall convene at the Under Secretary for Management’s discretion, and at such time as—

“(1) a new acquisition program is initiated;

“(2) a major acquisition program—

“(A) requires authorization to proceed from one acquisition decision event to another throughout the acquisition life-cycle;

“(B) is in breach of its approved acquisition program baseline; or

“(C) requires additional review, as determined by the Under Secretary for Management; or

“(3) a non-major acquisition program requires review, as determined by the Under Secretary for Management.

“(d) RESPONSIBILITIES.—The responsibilities of the Board are as follows:
“(1) Determine the appropriate acquisition level and acquisition decision authority for new acquisition programs based on the estimated eventual total expenditure of each such program to satisfy the mission need of the Department over the life-cycle of such acquisition regardless of funding source.

“(2) Determine whether a proposed acquisition has met the requirements of key phases of the acquisition life-cycle framework and is able to proceed to the next phase and eventual full production and deployment.

“(3) Oversee whether a proposed acquisition’s business strategy, resources, management, and accountability is executable and is aligned with the mission and strategic goals of the Department.

“(4) Support the person with acquisition decision authority for an acquisition in determining the appropriate direction for such acquisition at key acquisition decision events.

“(5) Conduct systematic reviews of acquisitions to ensure that such acquisitions are progressing in accordance with best practices and in compliance with the most recently approved documents for such acquisitions’ current acquisition phases.
“(6) Review the acquisition documents of each major acquisition program, including the acquisition program baseline and documentation reflecting consideration of tradeoffs among cost, schedule, and performance objectives, to ensure the reliability of underlying data.

“(7) Ensure that practices are adopted and implemented to require consideration of trade-offs among cost, schedule, and performance objectives as part of the process for developing requirements for major acquisition programs prior to the initiation of the second acquisition decision event, including, at a minimum, the following practices:

“(A) Department officials responsible for acquisition, budget, and cost estimating functions are provided with the appropriate opportunity to develop estimates and raise cost and schedule concerns before performance objectives are established for capabilities when feasible.

“(B) Full consideration is given to possible trade-offs among cost, schedule, and performance objectives for each alternative.

“(e) DOCUMENTATION.—

“(1) IN GENERAL.—The chair of the Board shall ensure that all actions and decisions made pur-
suant to the responsibilities of the Board under sub-
section (d) are documented in an acquisition decision
memorandum that includes—

“(A) a summary of the action at issue or
purpose for convening a meeting under sub-
section (c);

“(B) the decision with respect to actions
discussed during such meeting;

“(C) the rationale for such a decision, in-
cluding justifications for any such decision
made to allow acquisition programs to deviate
from the acquisition management policy of the
Department;

“(D) any assigned items for further action;
and

“(E) the signature of the chair verifying
the contents of such memorandum.

“(2) SUBMISSION OF MEMORANDUM.—Not later
than seven days after the date on which the acquisi-
tion decision memorandum is signed by the chair
pursuant to paragraph (1)(E), the chair shall submit
to the Secretary, the Committee on Homeland Secu-
rity of the House of Representatives, and the Com-
mittee on Homeland Security and Governmental Af-
fairs of the Senate a copy of such memorandum.
“(f) DEFINITIONS.—In this section:

“(1) ACQUISITION.—The term ‘acquisition’ has the meaning given such term in section 131 of title 41, United States Code.

“(2) ACQUISITION DECISION AUTHORITY.—The term ‘acquisition decision authority’ means the authority, held by the Secretary to—

“(A) ensure acquisition programs are in compliance with Federal law, the Federal Acquisition Regulation, and Department acquisition management directives;

“(B) review (including approving, pausing, modifying, or cancelling) an acquisition program through the life-cycle of such program;

“(C) ensure that acquisition program managers have the resources necessary to successfully execute an approved acquisition program;

“(D) ensure appropriate acquisition program management of cost, schedule, risk, and system performance of the acquisition program at issue, including assessing acquisition program baseline breaches and directing any corrective action for such breaches; and

“(E) ensure that acquisition program managers, on an ongoing basis, monitor cost, sched-
uile, and performance against established baselines and use tools to assess risks to an acquisition program at all phases of the life-cycle of such program to avoid and mitigate acquisition program baseline breaches.

“(3) Acquisition decision event.—The term ‘acquisition decision event’, with respect to an acquisition program, means a predetermined point within each of the acquisition phases at which the acquisition decision authority determines whether such acquisition program shall proceed to the next acquisition phase.

“(4) Acquisition decision memorandum.—The term ‘acquisition decision memorandum’ means the official documented record of decisions, including the rationale for such decisions and any assigned actions, for the acquisition at issue, as determined by the person exercising acquisition decision authority for such acquisition.

“(5) Acquisition program baseline.—The term ‘acquisition program baseline’, with respect to an acquisition program, means a summary of the cost, schedule, and performance parameters, expressed in standard, measurable, quantitative terms,
which must be satisfied to accomplish the goals of such program.

“(6) BEST PRACTICES.—The term ‘best practices’, with respect to acquisition, means a knowledge-based approach to capability development that includes—

“(A) identifying and validating needs;

“(B) assessing alternatives to select the most appropriate solution;

“(C) clearly establishing well-defined requirements;

“(D) developing realistic cost estimates and schedules that account for the entire life-cycle of such an acquisition;

“(E) securing stable funding that matches resources to requirements before initiating such development;

“(F) demonstrating technology, design, and manufacturing maturity before initiating production of the item that is the subject of such acquisition;

“(G) using milestones and exit criteria or specific accomplishments that demonstrate the attainment of knowledge to support progress;
“(H) regularly assessing and managing risks to achieving requirements and cost and schedule goals;

“(I) adopting and executing standardized processes with known success across programs;

“(J) establishing an adequate workforce that is qualified and sufficient to perform necessary functions; and

“(K) integrating the capabilities described in subparagraphs (A) through (J).

“(7) MAJOR ACQUISITION PROGRAM.—The term ‘major acquisition program’ means—

“(A) a Department capital asset, service, or hybrid acquisition program that is estimated by the Secretary to require an eventual total expenditure of at least $300 million (based on fiscal year 2022 constant dollars) over its life-cycle cost; or

“(B) a program identified by the Under Secretary for Management as a program of special interest.

“(8) NON-MAJOR ACQUISITION PROGRAM.—The term ‘non-major acquisition program’ means a Department capital asset, service, or hybrid acquisition program that is estimated by the Secretary to re-
quire an eventual total expenditure of less than $300,000,000 (based on fiscal year 2022 constant dollars) over its life-cycle.”.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is amended by inserting after the item relating to section 837 the following new item:

“Sec. 838. Acquisition Review Board.”.

SEC. 59127. DHS CONTRACT REPORTING.

(a) DAILY PUBLIC REPORT OF COVERED CONTRACT AWARDS.—

(1) IN GENERAL.—The Secretary shall post, maintain, and update in accordance with paragraph (2), on a publicly available website of the Department, a daily report of all covered contract awards. Each reported covered contract award shall include information relating to—

(A) the contract number, modification number, or delivery order number;

(B) the contract type;

(C) the amount obligated for such award;

(D) the total contract value for such award, including all options;

(E) the description of the purpose for such award;
(F) the number of proposals or bids received;

(G) the name and address of the vendor, and whether such vendor is considered a small business;

(H) the period and each place of performance for such award;

(I) whether such award is multiyear;

(J) whether such award requires a small business subcontracting plan; and

(K) the contracting office and the point of contact for such office.

(2) UPDATE.—Updates referred to in paragraph (1) shall occur not later than two business days after the date on which the covered contract is authorized or modified.

(3) SUBSCRIBING TO ALERTS.—The website referred to in paragraph (1) shall provide the option to subscribe to an automatic notification of the publication of each report required under such paragraph.

(4) EFFECTIVE DATE.—Paragraph (1) shall take effect on the date that is 180 days after the date of the enactment of this section.
(b) **UNDEFINITIZED CONTRACT ACTION OR DEFINITIZED AMOUNT.**—If a covered contract award reported pursuant to subsection (a) includes an undefinitized contract action, the Secretary shall—

(1) report the estimated total contract value for such award and the amount obligated upon award;

and

(2) once such award is definitized, update the total contract value and amount obligated.

(c) **EXEMPTION.**—Each report required under subsection (a) shall not include covered contract awards relating to classified products, programs, or services.

(d) **DEFINITIONS.**—In this section:

(1) **COVERED CONTRACT AWARD**.—The term “covered contract award”—

(A) means a contract action of the Department with the total authorized dollar amount of $4,000,000 or greater, including unexercised options; and

(B) includes—

(i) contract awards governed by the Federal Acquisition Regulation;

(ii) modifications to a contract award that increase the total value, expand the
scope of work, or extend the period of performance;

(iii) orders placed on a multiple award or multiple-agency contract that includes delivery or quantity terms that are indefinite;

(iv) other transaction authority agreements; and

(v) contract awards made with other than full and open competition.

(2) DEFINITIZED AMOUNT.—The term “definitized amount” means the final amount of a covered contract award after agreement between the Department and the contractor at issue.

(3) DEPARTMENT.—The term “Department” means the Department of Homeland Security.

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

(5) SMALL BUSINESS.—The term “small business” means an entity that qualifies as a small business concern, as such term is described under section 3 of the Small Business Act (15 U.S.C. 632).

(6) TOTAL CONTRACT VALUE.—The term “total contract value” means the total amount of funds expected to be provided to the contractor at issue
under the terms of the contract through the full pe-
riod of performance.

(7) UNDEFINITIZED CONTRACT ACTION.—The
term “undefinitized contract action” means any con-
tract action for which the contract terms, specifica-
tions, or price is not established prior to the start
of the performance of a covered contract award.

SEC. 59128. UNMANNED AERIAL SECURITY.

(a) Prohibition on Agency Operation or Pro-
curement.—Except as provided in subsection (b) and
subsection (c)(3), the Secretary of Homeland Security
may not operate, provide financial assistance for, or enter
into or renew a contract for the procurement of—

(1) an unmanned aircraft system (UAS) that—

(A) is manufactured in a covered foreign
country or by a corporation domiciled in a cov-
ered foreign country;

(B) uses flight controllers, radios, data
transmission devices, cameras, or gimbals man-
ufactured in a covered foreign country or by a
corporation domiciled in a covered foreign coun-
try;

(C) uses a ground control system or oper-
ating software developed in a covered foreign
country or by a corporation domiciled in a covered foreign country; or

(D) uses network connectivity or data storage located in a covered foreign country or administered by a corporation domiciled in a covered foreign country;

(2) a software operating system associated with a UAS that uses network connectivity or data storage located in a covered foreign country or administered by a corporation domiciled in a covered foreign country; or

(3) a system for the detection or identification of a UAS, which system is manufactured in a covered foreign country or by a corporation domiciled in a covered foreign country.

(b) WAIVER.—

(1) IN GENERAL.—The Secretary of Homeland Security is authorized to waive the prohibition under subsection (a) if the Secretary certifies in writing to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate that a UAS, a software operating system associated with a UAS, or a system for the detection or identification of a UAS referred to in any of subpara-
graphs (A) through (C) of such subsection that is
the subject of such a waiver is required—

(A) in the national interest of the United
States;

(B) for counter-UAS surrogate research,
testing, development, evaluation, or training; or

(C) for intelligence, electronic warfare, or
information warfare operations, testing, anal-
ysis, and or training.

(2) NOTICE.—The certification described in
paragraph (1) shall be submitted to the Committees
specified in such paragraph by not later than the
date that is 14 days after the date on which a waiv-
er is issued under such paragraph.

(c) EFFECTIVE DATES.—

(1) IN GENERAL.—This Act shall take effect on
the date that is 120 days after the date of the enact-
ment of this Act.

(2) WAIVER PROCESS.—Not later than 60 days
after the date of the enactment of this Act, the Sec-
retary of Homeland Security shall establish a proc-
ess by which the head of an office or component of
the Department of Homeland Security may request
a waiver under subsection (b).
(3) EXCEPTION.—Notwithstanding the prohibition under subsection (a), the head of an office or component of the Department of Homeland Security may continue to operate a UAS, a software operating system associated with a UAS, or a system for the detection or identification of a UAS described in any of subparagraphs (1) through (3) of such subsection that was in the inventory of such office or component on the day before the effective date of this Act until—

(A) such time as the Secretary of Homeland Security has—

(i) granted a waiver relating thereto under subsection (b); or

(ii) declined to grant such a waiver; or

(B) one year after the date of the enactment of this Act,

whichever is later.

(d) DRONE ORIGIN SECURITY REPORT TO CONGRESS.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Sen-
ate a terrorism threat assessment and report that contains information relating to the following:

(1) The extent to which the Department of Homeland Security has previously analyzed the threat that a UAS, a software operating system associated with a UAS, or a system for the detection or identification of a UAS from a covered foreign country operating in the United States poses, and the results of such analysis.

(2) The number of UAS, software operating systems associated with a UAS, or systems for the detection or identification of a UAS from a covered foreign country in operation by the Department, including an identification of the component or office of the Department at issue, as of such date.

(3) The extent to which information gathered by such a UAS, a software operating system associated with a UAS, or a system for the detection or identification of a UAS from a covered foreign country could be employed to harm the national or economic security of the United States.

(e) DEFINITIONS.—In this section:

(1) COVERED FOREIGN COUNTRY.—The term “covered foreign country” means a country that—
(A) the intelligence community has identified as a foreign adversary in its most recent Annual Threat Assessment; or

(B) the Secretary of Homeland Security, in coordination with the Director of National Intelligence, has identified as a foreign adversary that is not included in such Annual Threat Assessment.

(2) INTELLIGENCE COMMUNITY.—The term “intelligence community” has the meaning given such term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

(3) UNMANNED AIRCRAFT SYSTEM; UAS.—The terms “unmanned aircraft system” and “UAS” have the meaning given the term “unmanned aircraft system” in section 44801 of title 49, United States Code.

Subtitle C—Enhancing DHS Operations

SEC. 59131. QUADRENNIAL HOMELAND SECURITY REVIEW TECHNICAL CORRECTIONS.

(a) In General.—Section 707 of the Homeland Security Act of 2002 (6 U.S.C. 347) is amended—

(1) in subsection (a)(3)—
(A) in subparagraph (B), by striking “and” after the semicolon at the end;

(B) by redesignating subparagraph (C) as subparagraph (D); and

(C) by inserting after subparagraph (B) the following new subparagraph:

“(C) representatives from appropriate advisory committees established pursuant to section 871, including the Homeland Security Advisory Council and the Homeland Security Science and Technology Advisory Committee, or otherwise established, including the Aviation Security Advisory Committee established pursuant to section 44946 of title 49, United States Code; and”;

(2) in subsection (b)—

(A) in paragraph (2), by inserting before the semicolon at the end the following: “based on the risk assessment required pursuant to subsection (c)(2)(B)”;

(B) in paragraph (3)—

(i) by inserting “, to the extent practicable,” after “describe”; and

(ii) by striking “budget plan” and inserting “resources required”;
(C) in paragraph (4)—

(i) by inserting “, to the extent practicable,” after “identify”;

(ii) by striking “budget plan required to provide sufficient resources to successfully” and inserting “resources required to”; and

(iii) by striking the semicolon at the end and inserting the following: “, including any resources identified from redundant, wasteful, or unnecessary capabilities or capacities that may be redirected to better support other existing capabilities or capacities, as the case may be; and”;

(D) in paragraph (5), by striking “; and” and inserting a period; and

(E) by striking paragraph (6);

(3) in subsection (c)—

(A) in paragraph (1), by striking “December 31 of the year” and inserting “60 days after the date of the submission of the President’s budget for the fiscal year after the fiscal year”; and

(B) in paragraph (2)—
(i) in subparagraph (B), by striking “description of the threats to” and inserting “risk assessment of”; 
(ii) in subparagraph (C), by inserting “, as required under subsection (b)(2)” before the semicolon at the end; 
(iii) in subparagraph (D)—
   (I) by inserting “to the extent practicable,” before “a description”; and 
   (II) by striking “budget plan” and inserting “resources required”; 
(iv) in subparagraph (F)—
   (I) by inserting “to the extent practicable,” before “a discussion”; 
   and 
   (II) by striking “the status of”; 
(v) in subparagraph (G)—
   (I) by inserting “to the extent practicable,” before “a discussion”; 
   (II) by striking “the status of”; 
   (III) by inserting “and risks” before “to national homeland”; and 
   (IV) by inserting “and” after the semicolon at the end;
(vi) by striking subparagraph (II); and

(vii) by redesignating subparagraph (I) as subparagraph (II); (C) by redesignating paragraph (3) as paragraph (4); and

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

“(3) DOCUMENTATION.—The Secretary shall retain and, upon request, provide to Congress the following documentation regarding each quadrennial homeland security review:

“(A) Records regarding the consultation carried out pursuant to subsection (a)(3), including the following:

“(i) All written communications, including communications sent out by the Secretary and feedback submitted to the Secretary through technology, online communications tools, in-person discussions, and the interagency process.

“(ii) Information on how feedback received by the Secretary informed each such quadrennial homeland security review.
“(B) Information regarding the risk assessment required pursuant to subsection (c)(2)(B), including the following:

“(i) The risk model utilized to generate such risk assessment.

“(ii) Information, including data used in the risk model, utilized to generate such risk assessment.

“(iii) Sources of information, including other risk assessments, utilized to generate such risk assessment.

“(iv) Information on assumptions, weighing factors, and subjective judgments utilized to generate such risk assessment, together with information on the rationale or basis thereof.”;

(4) by redesignating subsection (d) as subsection (e); and

(5) by inserting after subsection (c) the following new subsection:

“(d) REVIEW.—Not later than 90 days after the submission of each report required under subsection (c)(1), the Secretary shall provide to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs
of the Senate information on the degree to which the find-
ings and recommendations developed in the quadrennial
homeland security review that is the subject of such report
were integrated into the acquisition strategy and expendi-
ture plans for the Department.”.

(b) EFFECTIVE DATE.—The amendments made by
this Act shall apply with respect to a quadrennial home-
land security review conducted after December 31, 2021.

SEC. 59132. BOMBING PREVENTION.

(a) OFFICE FOR BOMBING PREVENTION.—

(1) IN GENERAL.—Title XXII of the Homeland
Security Act of 2002 (6 U.S.C. 651 et seq.) is
amended by adding at the end the following new
subtitle:

“Subtitle E—Bombing Prevention

“SEC. 2251. OFFICE FOR BOMBING PREVENTION.

“(a) ESTABLISHMENT.—There is established within
the Department an Office for Bombing Prevention (in this
section referred to as the ‘Office’).

“(b) ACTIVITIES.—The Office shall have the primary
responsibility within the Department for enhancing the
ability and coordinating the efforts of the United States
to deter, detect, prevent, protect against, mitigate, and re-
spond to terrorist explosive threats and attacks in the
United States, including by carrying out the following:
“(1) Advising the Secretary on matters related to terrorist explosive threats and attacks in the United States.

“(2) Coordinating the efforts of the Department to counter terrorist explosive threats and attacks in the United States, including by carrying out the following:

“(A) Developing, in coordination with the Under Secretary for Strategy, Policy, and Plans, the Department’s strategy against terrorist explosives threats and attacks, including efforts to support the security and preparedness of critical infrastructure and the public sector and private sector.

“(B) Leading the prioritization of the Department’s efforts against terrorist explosive threats and attacks, including preparedness and operational requirements.

“(C) Ensuring, in coordination with the Under Secretary for Science and Technology and the Administrator of the Federal Emergency Management Agency, the identification, evaluation, and availability of effective technology applications through field pilot testing and acquisition of such technology applications
by the public sector to deter, detect, prevent, protect against, mitigate, and respond to terrorist explosive threats and attacks in the United States.

“(D) Providing advice and recommendations to the Administrator of the Federal Emergency Management Agency regarding the effective use of grants authorized under section 2002.

“(E) In coordination with the Assistant Secretary for Countering Weapons of Mass Destruction, aligning Department efforts related to terrorist explosive threats and attacks in the United States and weapons of mass destruction.

“(3) Engaging other Federal departments and agencies, including Sector Risk Management Agencies, regarding terrorist explosive threats and attacks in the United States.

“(4) Facilitating information sharing and decision support of the public and private sector involved in deterrence, detection, prevention, protection against, mitigation of, and response to terrorist explosive threats and attacks in the United States.

Such sharing and support may include the following:
“(A) Operating and maintaining a secure information sharing system that allows the sharing of critical information and data relating to terrorist explosive attack tactics, techniques, procedures, and security capabilities, including information and data described in paragraph (6) and section 2242.

“(B) Working with international partners, in coordination with the Office for International Affairs of the Department, to develop and share effective practices to deter, prevent, detect, protect against, mitigate, and respond to terrorist explosive threats and attacks in the United States.

“(5) Promoting security awareness among the public and private sector and the general public regarding the risks posed by the misuse of explosive precursor chemicals and other bomb-making materials.

“(6) Providing training, guidance, assessments, and planning assistance to the public and private sector, as appropriate, to help counter the risk of terrorist explosive threats and attacks in the United States.
“(7) Conducting analysis and planning for the capabilities and requirements necessary for the public and private sector, as appropriate, to deter, detect, prevent, protect against, mitigate, and respond to terrorist explosive threats and attacks in the United States by carrying out the following:

“(A) Maintaining a database on capabilities and requirements, including capabilities and requirements of public safety bomb squads, explosive detection canine teams, special tactics teams, public safety dive teams, and recipients of services described in section 2242.

“(B) Applying the analysis derived from the database described in subparagraph (A) with respect to the following:

“(i) Evaluating progress toward closing identified gaps relating to national strategic goals and standards related to deterring, detecting, preventing, protecting against, mitigating, and responding to terrorist explosive threats and attacks in the United States.

“(ii) Informing decisions relating to homeland security policy, assistance, training, research, development efforts, testing
and evaluation, and related requirements regarding deterring, detecting, preventing, protecting against, mitigating, and responding to terrorist explosive threats and attacks in the United States.

“(8) Promoting secure information sharing of sensitive material and promoting security awareness, including by carrying out the following:

“(A) Operating and maintaining a secure information sharing system that allows the sharing among and between the public and private sector of critical information relating to explosive attack tactics, techniques, and procedures.

“(B) Educating the public and private sectors about explosive precursor chemicals.

“(C) Working with international partners, in coordination with the Office for International Affairs of the Department, to develop and share effective practices to deter, detect, prevent, protect against, mitigate, and respond to terrorist explosive threats and attacks in the United States.

“(D) Executing national public awareness and vigilance campaigns relating to terrorist ex-
plosive threats and attacks in the United States, preventing explosive attacks, and activities and measures underway to safeguard the United States.

“(E) Working with relevant stakeholder organizations.

“(9) Providing any other assistance the Secretary determines necessary.

“SEC. 2252. COUNTERING EXPLOSIVE DEVICES TECHNICAL ASSISTANCE.

“(a) Establishment.—Upon request, the Secretary shall, to the extent practicable, provide to the public and private sector technical assistance services to support the security and preparedness of such sectors, as appropriate, to counter terrorist explosive threats and attacks that pose a risk in certain jurisdictions, including vulnerable and disadvantaged communities, to critical infrastructure facilities, or to special events, as appropriate.

“(b) Elements.—Technical assistance services provided pursuant to subsection (a) shall—

“(1) support the planning and implementation of effective measures to deter, detect, prevent, protect against, mitigate, and respond to terrorist explosive threats and attacks in the United States, in-
114

including effective strategic risk management and
emergency operations plans;

“(2) support the security of explosive precursor
chemicals and other bomb-making materials outside
of regulatory control;

“(3) support efforts to prepare for and respond
to bomb threats or other acts involving the malicious
conveyance of false information concerning terrorist
explosive threats and attacks in the United States;

“(4) make available resources to enhance deter-
rence, prevention, detection, protection, mitigation,
and response capabilities for terrorist explosive
threats and attacks in the United States, including
coordination and communication, to better integrate
State, local, Tribal, and territorial and private sector
capabilities and assets, as appropriate, with Federal
operations;

“(5) make available augmenting resources, as
appropriate, to enable State, local, Tribal, and terri-
torial governments to sustain and refresh their capa-
bilities;

“(6) track performance in meeting the goals
and associated plans of the provision of such tech-
nical assistance; and
“(7) include any other assistance the Secretary
determines necessary.

“SEC. 2253. RELATIONSHIP TO OTHER DEPARTMENT COM-
ONENTS AND FEDERAL AGENCIES.

“(a) IN GENERAL.—The authority of the Secretary
under this subtitle shall not affect or diminish the author-
ity or the responsibility of any officer of any other Federal
agency with respect to the command, control, or direction
of the functions, personnel, funds, assets, or liabilities of
any other such Federal agency.

“(b) DEPARTMENT COMPONENTS.—Nothing in this
subtitle or any other provision of law may be construed
to affect or reduce the responsibilities of—

“(1) the Countering Weapons of Mass Destruc-
tion Office or the Assistant Secretary of the Office,
including with respect to any asset, function, or mis-
ion of the Office or the Assistant Secretary, as the
case may be;

“(2) the Federal Emergency Management
Agency or the Administrator of the Agency, includ-
ing the diversion of any asset, function, or mission
of the Agency or the Administrator as the case may
be; or

“(3) the Transportation Security Administra-
tion or the Administrator of the Administration, in-
1. including the diversion of any asset, function, or mission of the Administration or the Administrator, as the case may be.”.

(2) Strategy and Reports.—

(A) Strategy.—Not later than one year after the date of the enactment of this section, the head of the Office for Bombing Prevention of the Department of Homeland Security (established pursuant to section 2241 of the Homeland Security Act of 2002, as added by paragraph (1)), in consultation with the heads of other components of the Department and the heads of other Federal agencies, as appropriate, shall develop a strategy to align the Office’s activities with the threat environment and stakeholder needs, and make the public and private sector aware of the Office’s capabilities. Such strategy shall include the following elements:

   (i) Information on terrorist explosive threats, tactics, and attacks in the United States.

   (ii) Information, by region of the United States, regarding public and private sector entities likely to be targeted by terrorist explosive threats and attacks in
the United States, including historically
black colleges and universities and minor-
ity serving institutions, places of worship,
health care facilities, transportation sys-
tems, commercial facilities, and govern-
ment facilities.

(iii) Guidance on how outreach to
owners and operators of critical infrastruc-
ture (as such term is defined in section
1016(e) of Public Law 107–56 (42 U.S.C.
5195e(e))) in a region should be
prioritized.

(iv) A catalogue of the services and
training currently offered by the Office,
and a description of how such services and
trainings assist the public and private sec-
tor to deter, detect, prevent, protect
against, mitigate, and respond to terrorist
explosive threats and attacks in the United
States.

(v) Long-term objectives of the Office,
including future service and training offer-
ings.
(vi) Metrics for measuring the effectiveness of services and trainings offered by the Office.

(vii) An assessment of resource requirements necessary to implement such strategy.

(viii) A description of how the Office partners with other components of the Department and other Federal agencies to carry out its mission.

(B) REPORTS.—Not later than one year after the date of the enactment of this section and annually thereafter, the Secretary of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report describing the activities of the Office for Bombing Prevention of the Department of Homeland Security (established pursuant to section 2241 of the Homeland Security Act of 2002, as added by paragraph (1)). Each such report shall include information on the following:
(i) Changes to terrorist explosive threats, tactics, and attacks in the United States.

(ii) Changes to the types of public and private sector entities likely to be targeted by terrorist explosive threats and attacks in the United States.

(iii) The number of trainings, assessments, and other engagements carried out by the Office within each region of the United States, including a description of the critical infrastructure sector or stakeholder served.

(iv) The number of trainings, assessments, or other engagements the Office was asked to conduct but did not, and an explanation relating thereto.

(v) The effectiveness of the trainings, assessments, or other engagements provided by the Office based on the metrics described in subparagraph (A)(vi).

(vi) Any changes or anticipated changes in the trainings, assessments, and other engagements, or any other services,
offered by the Office, and an explanation relating thereto.

(3) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 2246 the following new items:

“Subtitle E—Bombing Prevention

“Sec. 2251. Office for Bombing Prevention.
“Sec. 2252. Countering explosive devices technical assistance.
“Sec. 2253. Relationship to other Department components and Federal agencies.”.

(b) EXPLOSIVES TECHNOLOGY DEVELOPMENT.—

(1) 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. EXPLOSIVES RESEARCH AND DEVELOPMENT.

“(a) IN GENERAL.—The Secretary, acting through the Under Secretary for Science and Technology, and in coordination with the head of the Office for Bombing Prevention and the Assistant Secretary for the Countering Weapons of Mass Destruction Office, and in consultation with the Attorney General, the Secretary of Defense, and the head of any other relevant Federal department or agency, including Sector Risk Management Agencies, shall ensure coordination and information sharing regarding nonmilitary research, development, testing, and evaluation
activities of the Federal Government relating to the deter-
rence, detection, prevention, protection against, mitigation
of, and response to terrorist explosive threats and attacks
in the United States.

“(b) LEVERAGING MILITARY RESEARCH.—The Sec-
retary, acting through the Under Secretary for Science
and Technology, and in coordination with the head of the
Office for Bombing Prevention and the Assistant Sec-
retary for the Countering of Weapons of Mass Destruction
Office, shall consult with the Secretary of Defense and the
head of any other relevant Federal department or agency,
including Sector Risk Management Agencies, to ensure
that, to the maximum extent possible, military policies and
procedures, and research, development, testing, and eval-
uation activities relating to the deterrence, detection, pre-
vention, protection against, mitigation of, and response to
terrorist explosive threats and attacks in the United
States are adapted to nonmilitary uses.”

(2) CLERICAL AMENDMENT.—The table of con-
tents in section 1(b) of the Homeland Security Act
of 2002 is amended by inserting after the item relat-
ing to section 323 the following new item:

“Sec. 324. Explosives research and development.”
SEC. 59133. DHS BASIC TRAINING ACCREDITATION IMPROVEMENT.

(a) Reporting on Basic Training Programs of the Department of Homeland Security.—

(1) Annual reporting.—

(A) In general.—Not later than 90 days after the date of the enactment of this Act and annually thereafter, the Secretary of Homeland Security shall report to the relevant congressional committees on the accreditation status for each basic training program within the Department of Homeland Security, including information relating to the following:

(i) The date on which each such program achieved initial accreditation, or in the case of a program that is not currently accredited, the reasons for not obtaining or maintaining accreditation, the activities, if any, taken to achieve accreditation, and an anticipated timeline for accreditation of such program.

(ii) The date each such program most recently received accreditation or reaccreditation, if applicable.

(iii) Each such program’s anticipated accreditation or next reaccreditation date.
(iv) The name of the accreditation manager for each such program.

(B) Termination of Reporting Requirement.—Annual reports under subparagraph (A) shall terminate when all basic training programs of the Department of Homeland Security are accredited.

(2) Lapse in Accreditation.—

(A) In General.—If a basic training program of the Department of Homeland Security loses accreditation, the head of the relevant component of the Department shall notify the Secretary of Homeland Security not later than 30 days after such loss.

(B) Notice to Congress.—Not later than 30 days after receiving a notification pursuant to subparagraph (A), the Secretary of Homeland Security shall notify the relevant congressional committees of the lapse in accreditation at issue, the reason for such lapse, and the activities underway and planned to regain accreditation.

(3) Definitions.—In this section:

(A) Accreditation.—The term “accreditation” means the recognition by a board that
a basic training program is administered, developed, and delivered according to an applicable set of standards.

(B) ACCREDITATION MANAGER.—The term “accreditation manager” means the individual assigned by the component of the Department of Homeland Security to manage accreditation activities for a basic training program.

(C) BASIC TRAINING PROGRAM.—The term “basic training program” means an entry level program of the Department of Homeland Security that is transitional to law enforcement service, provides training on critical competencies and responsibilities, and is typically a requirement for appointment to a law enforcement service job or job series.

(D) REACCREDITATION.—The term “re-accreditation” means the assessment of a basic training program after initial accreditation to ensure the continued compliance with an applicable set of standards.

(E) RELEVANT CONGRESSIONAL COMMITTEES.—The term “relevant congressional committees” means the Committee on Homeland Security and the Committee on the Judiciary of
the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee of the Judiciary of the Senate.

(b) **Research and Development.**—The Under Secretary for Science and Technology of the Department of Homeland Security shall carry out research and development of systems and technologies to enhance access to training offered by the Federal Law Enforcement Training Centers to State, local, Tribal, and territorial law enforcement, with particular attention to law enforcement in rural and remote communities, for the purpose of enhancing domestic preparedness for and collective response to terrorism and other homeland security threats.

SEC. 59134. DEPARTMENT OF HOMELAND SECURITY INSPECTOR GENERAL TRANSPARENCY.

(a) **In General.**—Subtitle B of title VIII of the Homeland Security Act of 2002 is amended by inserting before section 812 the following new section:

```
SEC. 811. OFFICE OF INSPECTOR GENERAL.

“(a) Publication of Reports.—

“(1) In General.—Beginning not later than 30 days after the date of the enactment of this section, the Inspector General of the Department shall submit to the appropriate congressional committees
any report finalized on and after such date that substantiates—

“(A) a violation of paragraph (8) or (9) of section 2302(b) of title 5, United States Code, section 1034 of title 10, United States Code, or Presidential Personnel Directive-19; or

“(B) an allegation of misconduct, waste, fraud, abuse, or violation of policy within the Department involving a member of the Senior Executive Service or politically appointed official of the Department.

“(2) PUBLIC AVAILABILITY.—

“(A) IN GENERAL.—Concurrent with the submission to the appropriate congressional committees of reports pursuant to paragraph (1), the Inspector General shall, consistent with privacy, civil rights, and civil liberties protections, publish on a publicly available website of the Inspector General each such report.

“(B) EXCEPTION.—The requirement pursuant to subparagraph (A) to publish reports does not apply if section (5)(e)(1) of the Inspector General Act of 1978 applies to any such report.

“(3) REQUIREMENT.—
“(A) IN GENERAL.—The Inspector General of the Department may not redact any portion of a report submitted pursuant to paragraph (1).

“(B) EXCEPTION.—The requirement under subparagraph (A) shall not apply with respect to the name or any other identifying information, including any contextual details not relevant to the audit, inspection, or evaluation at issue that may be used by other employees or officers of the Department to determine the identity of a whistleblower complainant, of a whistleblower complainant who does not consent to the inclusion of such in a report of the Inspector General.

“(b) SEMIANNUAL REPORTING.—Beginning with the first semiannual report transmitted to the appropriate committees or subcommittees of the Congress pursuant to section 5(b) of the Inspector General Act of 1978 that is transmitted after the date of the enactment of this section, each such report shall be accompanied by a list of ongoing audits, inspections, and evaluations of the Department, together with a narrative description relating to each such audit, inspection, or evaluation that identifies the scope of such audit, inspection, or evaluation, as the
case may be, as well as the subject office, component, or
directorate of the Department. For each such ongoing
audit, inspection, or evaluation such narrative description
shall include the following:

“(1) Information relating to the source of each
such audit, inspection, or evaluation.

“(2) Information regarding whether each such
audit, inspection, or evaluation is being conducted
independently, jointly, concurrently, or in some other
manner.

“(3) In the event each such audit, inspection, or
evaluation was initiated due to a referral, the date
on which the Inspector General notified the origi-
nator of a referral of the Inspector General’s inten-
tion to carry out such audit, inspection, or evalua-
tion.

“(4) Information relating to the dates on
which—

“(A) each such audit, inspection, or eval-
uation was initiated;

“(B) a draft report relating to each such
audit, inspection, or evaluation is scheduled to
be submitted to the Secretary for review; and

“(C) a final report relating to each such
audit, inspection, or evaluation is scheduled to
be submitted to the appropriate congressional committees and published on the website of the Inspector General in accordance with paragraphs (1) and (2), respectively, of subsection (a).

“(5) An explanation for—

“(A) any significant changes to the narrative description of each such audit, inspection, or evaluation, including the identification of the subject office, component, or directorate of the Department; or

“(B) a delay of more than 30 days in the scheduled date for submitting to the Secretary a draft report for review or publishing on the website of the Inspector General of the Department the final report relating to each such audit, inspection, or evaluation.

“(6) Data regarding tips and complaints made to the Inspector General Hotline of the Department or otherwise referred to the Department, including—

“(A) the number and type of tips and complaints regarding fraud, waste, abuse, corruption, financial crimes, civil rights and civil liberty abuse, or other complaints regarding crimi-
nal or non-criminal activity associated with fraud, waste, or abuse;

“(B) actions taken by the Department to address or resolve each substantiated tip or complaint;

“(C) the total amount of time it took the Department to so address or resolve each such substantiated tip or complaint;

“(D) the total number of tips and complaints that are substantiated compared with the number of tips and complaints that are unsubstantiated; and

“(E) the percentage of audits, inspections, and evaluations that are initiated as a result of tips and complaints made to the Inspector General Hotline.

“(c) NOTIFICATION TO CONGRESS.—The Inspector General of the Department shall notify the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate if the head of an office or component of the Department does not provide in a timely manner to the Inspector General information or assistance that is requested by the Inspector General to conduct an audit, inspection, or evaluation.
“(d) DEFINITION.—In this section, the term ‘appropriate congressional committees’ means the Committee on Homeland Security of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and any committee of the House of Representatives or the Senate, respectively, having legislative or oversight jurisdiction under the Rules of the House of Representatives or the Senate, respectively, over the matter concerned.”.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by amending the item relating to section 811 to read as follows:

“Sec. 811. Office of Inspector General.”.

(c) REPORTS.—

(1) INSPECTOR GENERAL OF DHS.—Not later than one year after the date of the enactment of this Act, the Inspector General of the Department of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Comptroller General of the United States a report on the policies, procedures, and internal controls established that ensure compliance with the Quality Standards for Federal Offices of Inspector General from the
132  Council of Inspectors General on Integrity and Efficiency.

(2) **COMPTROLLER GENERAL.**—Not later than one year after receipt of the report required under paragraph (1), the Comptroller General of the United States shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate an evaluation of such report.

SEC. 59135. **PRESIDENT’S CUP CYBERSECURITY COMPETITION.**

(a) **IN GENERAL.**—The Director of the Cybersecurity and Infrastructure Security Agency (in this section referred to as the “Director”) of the Department of Homeland Security is authorized to hold an annual cybersecurity competition to be known as the “Department of Homeland Security Cybersecurity and Infrastructure Security Agency’s President’s Cup Cybersecurity Competition” (in this section referred to as the “competition”) for the purpose of identifying, challenging, and competitively awarding prizes, including cash prizes, to the United States Government’s best cybersecurity practitioners and teams across offensive and defensive cybersecurity disciplines.
(b) COMPETITION DESIGN.—

(1) IN GENERAL.—Notwithstanding section 1342 of title 31, United States Code, the Director, in carrying out the competition, may consult with, and consider advice from, any person who has experience or expertise in the development, design, or execution of cybersecurity competitions.

(2) LIMITATION.—The Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to consultations pursuant to this section.

(3) PROHIBITION.—A person with whom the Director consults under paragraph (1) may not—

(A) receive pay by reason of being so consulted; or

(B) be considered an employee of the Federal Government by reason of so consulting.

(c) ELIGIBILITY.—To be eligible to participate in the competition, an individual shall be a Federal civilian employee or member of the uniformed services (as such term is defined in section 2101(3) of title 5, United States Code) and shall comply with any rules promulgated by the Director regarding the competition.

(d) COMPETITION ADMINISTRATION.—The Director may enter into a grant, contract, cooperative agreement, or other agreement with a private sector for-profit or non-
profit entity or State or local government agency to administer the competition.

(c) COMPETITION PARAMETERS.—Each competition shall incorporate the following elements:

(1) Cybersecurity skills outlined in the National Initiative for Cybersecurity Education Framework, or any successor framework.

(2) Individual and team events.

(3) Categories demonstrating offensive and defensive cyber operations, such as software reverse engineering and exploitation, network operations, forensics, big data analysis, cyber analysis, cyber defense, cyber exploitation, secure programming, obfuscated coding, or cyber-physical systems.

(4) Any other elements related to paragraphs (1), (2), or (3) as determined necessary by the Director.

(f) USE OF FUNDS.—

(1) IN GENERAL.—Notwithstanding any other provision of law, the Director may use amounts made available to the Director for the competition for the following:

(A) Advertising, marketing, and promoting the competition.
(B) Meals for participants and organizers of the competition if attendance at the meal during the competition is necessary to maintain the integrity of the competition.

(C) Promotional items, including merchandise and apparel.

(D) Monetary and nonmonetary awards for competition participants, including members of the uniformed services.

(E) Necessary expenses for the honorary recognition of competition participants, including members of the uniformed services.

(F) Any other appropriate activity necessary to carry out the competition, as determined by the Director.

(2) APPLICATION.—This subsection shall apply to amounts appropriated on or after the date of the enactment of this Act.

(g) PRIZE LIMITATION.—The Director may make one or more awards per competition, except that the amount or value of each shall not exceed $10,000. The Secretary of Homeland Security may make one or more awards per competition, except the amount or the value of each shall not to exceed $25,000. A monetary award under this section shall be in addition to the regular pay of the recipient.
(h) REPORTING REQUIREMENTS.—The Director shall annually provide to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report that includes the following:

(1) A description of available funds under subsection (f) for each competition conducted in the preceding year.

(2) A description of expenditures authorized in subsection (g) for each competition.

(3) Information relating to the participation of each competition.

(4) Information relating to lessons learned from each competition and how such lessons may be applied to improve cybersecurity operations and recruitment of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security.

SEC. 59136. INDUSTRIAL CONTROL SYSTEMS CYBERSECURITY TRAINING.

(a) IN GENERAL.—Subtitle A of title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended by adding at the end the following new section:
SEC. 2220E. INDUSTRIAL CONTROL SYSTEMS CYBERSECURITY TRAINING INITIATIVE.

(a) Establishment.—

(1) In general.—The Industrial Control Systems Cybersecurity Training Initiative (in this section referred to as the ‘Initiative’) is established within the Agency.

(2) Purpose.—The purpose of the Initiative is to develop and strengthen the skills of the cybersecurity workforce related to securing industrial control systems.

(b) Requirements.—In carrying out the Initiative, the Director shall—

(1) ensure the Initiative includes—

(A) virtual and in-person trainings and courses provided at no cost to participants;

(B) trainings and courses available at different skill levels, including introductory level courses;

(C) trainings and courses that cover cyber defense strategies for industrial control systems, including an understanding of the unique cyber threats facing industrial control systems and the mitigation of security vulnerabilities in industrial control systems technology; and
“(D) appropriate consideration regarding
the availability of trainings and courses in dif-
ferent regions of the United States; and
“(2) engage in—
“(A) collaboration with the National Lab-
oratories of the Department of Energy in ac-
cordance with section 309;
“(B) consultation with Sector Risk Man-
agement Agencies; and
“(C) as appropriate, consultation with pri-
ivate sector entities with relevant expertise, such
as vendors of industrial control systems tech-
nologies.
“(c) REPORTS.—
“(1) IN GENERAL.—Not later than one year
after the date of the enactment of this section and
annually thereafter, the Director shall submit to the
Committee on Homeland Security of the House of
Representatives and the Committee on Homeland
Security and Governmental Affairs of the Senate a
report on the Initiative.
“(2) CONTENTS.—Each report under para-
graph (1) shall include the following:
“(A) A description of the courses provided
under the Initiative.
“(B) A description of outreach efforts to raise awareness of the availability of such courses.

“(C) Information on the number and demographics of participants in such courses, including by gender, race, and place of residence.

“(D) Information on the participation in such courses of workers from each critical infrastructure sector.

“(E) Plans for expanding access to industrial control systems education and training, including expanding access to women and underrepresented populations, and expanding access to different regions of the United States.

“(F) Recommendations on how to strengthen the state of industrial control systems cybersecurity education and training.”.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 2220D the following new item:

“Sec. 2220E. Industrial Control Systems Cybersecurity Training Initiative.”.
SEC. 59137. TSA REACHING ACROSS NATIONALITIES, SOCIETIES, AND LANGUAGES TO ADVANCE TRAVELER EDUCATION.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration (TSA) shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a plan to ensure that TSA material disseminated in major airports can be better understood by more people accessing such airports.

(b) CONTENTS.—The plan required under subsection (a) shall include the following:

(1) An identification of the most common languages other than English that are the primary languages of individuals that travel through or work in each major airport.

(2) A plan to improve—

(A) TSA materials to communicate information in languages identified pursuant to paragraph (1); and

(B) the communication of TSA material to individuals with vision or hearing impairments or other possible barriers to understanding such material.
(c) CONSIDERATIONS.—In developing the plan required under subsection (a), the Administrator of the TSA, acting through the Office of Civil Rights and Liberties, Ombudsman, and Traveler Engagement of the TSA, shall take into consideration data regarding the following:

(1) International enplanements.

(2) Local populations surrounding major airports.

(3) Languages spoken by members of Indian Tribes within each service area population in which a major airport is located.

(d) IMPLEMENTATION.—Not later than 180 days after the submission of the plan required under subsection (a), the Administrator of the TSA, in consultation with the owner or operator of each major airport, shall implement such plan.

(e) GAO REVIEW.—Not later than one year after the implementation pursuant to subsection (d) of the plan required under subsection (a), the Comptroller General of the United States shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a review of such implementation.

(f) DEFINITIONS.—In this section:
(1) AIRPORT.—The term “airport” has the meaning given such term in section 40102 of title 49, United States Code.

(2) INDIAN TRIBE.—The term “Indian Tribe” means an Indian Tribe, as such term is defined in section 102 of the Federally Recognized Indian Tribe List Act of 1994 (25 U.S.C. 5130), individually identified (including parenthetically) in the list published most recently as of the date of the enactment of this Act pursuant to section 104 of that Act (25 U.S.C. 5131).

(3) MAJOR AIRPORTS.—The term “major airports” means Category X and Category I airports.

(4) NON-TRAVELING INDIVIDUAL.—The term “non-traveling individual” has the meaning given such term in section 1560.3 of title 49, Code of Federal Regulations.

(5) TSA MATERIAL.—The term “TSA material” means signs, videos, audio messages, websites, press releases, social media postings, and other communications published and disseminated by the Administrator of the TSA in Category X and Category I airports for use by both traveling and non-traveling individuals.
SEC. 59138. BEST PRACTICES RELATED TO CERTAIN INFORMATION COLLECTED BY RENTAL COMPANIES AND DEALERS (DARREN DRAKE).

(a) DEVELOPMENT AND DISSEMINATION.—

(1) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Secretary of Homeland Security shall develop and disseminate best practices for rental companies and dealers to report suspicious behavior to law enforcement agencies at the point of sale of a covered rental vehicle.

(2) CONSULTATION; UPDATES.—The Secretary shall develop and, as necessary, update the best practices described in paragraph (1) after consultation with Federal, State, local, and Tribal law enforcement agencies and relevant transportation security stakeholders.

(3) GUIDANCE ON SUSPICIOUS BEHAVIOR.—The Secretary shall include, in the best practices developed under paragraph (1), guidance on defining and identifying suspicious behavior in a manner that protects civil rights and civil liberties.

(b) REPORT TO CONGRESS.—Not later than one year after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to Congress a report...
on the implementation of this section, including an assessment of—

(1) the impact of the best practices described in subsection (a) on efforts to protect the United States against terrorist attacks; and

(2) ways to improve and expand cooperation and engagement between—

(A) the Department of Homeland Security;

(B) Federal, State, local, and Tribal law enforcement agencies; and

(C) rental companies, dealers, and other relevant rental industry stakeholders.

c) DEFINITIONS.—In this section:

(1) The terms “dealer” and “rental company” have the meanings given those terms in section 30102 of title 49, United States Code.

(2) The term “covered rental vehicle” means a motor vehicle that—

(A) is rented without a driver for an initial term of less than 4 months; and

(B) is part of a motor vehicle fleet of 35 or more motor vehicles that are used for rental purposes by a rental company.

SEC. 59139. ONE-STOP PILOT PROGRAM.

(a) DEFINITIONS.—In this section:
(1) ADMINISTRATOR.—The term “Administrator” means the Administrator of the Transportation Security Administration.

(2) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term “appropriate congressional committees” means—

(A) the Committee on Homeland Security of the House of Representatives; and

(B) the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate.

(3) TSA.—The term “TSA” means the Transportation Security Administration of the Department of Homeland Security.

(b) ESTABLISHMENT.—Notwithstanding 44901(a) of title 49, United States Code, the Administrator, in coordination with the Commissioner of U.S. Customs and Border Protection, may establish a pilot program at not more than six foreign last point of departure airports to permit passengers and their accessible property arriving on direct flights or flight segments originating at such participating foreign airports to continue on additional flights or flight segments originating in the United States without additional security re-screening if—
(1) the initial screening was conducted in accordance with an aviation security screening agreement described in subsection (e);

(2) passengers arriving from participating foreign airports are unable to access their checked baggage until the arrival at their final destination; and

(3) upon arrival in the United States, passengers arriving from participating foreign airports do not come into contact with other arriving international passengers, those passengers’ property, or other persons who have not been screened or subjected to other appropriate security controls required for entry into the airport’s sterile area.

(c) REQUIREMENTS FOR PILOT PROGRAM.—In carrying out this section, the Administrator shall ensure that there is no reduction in the level of security or specific TSA aviation security standards or requirements for screening passengers and their property prior to boarding an international flight bound for the United States, including specific aviation security standards and requirements regarding—

(1) high risk passengers and their property;

(2) weapons, explosives, and incendiaries;

(3) screening passengers and property transferring at a foreign last point of departure airport from
another airport and bound for the United States,
and addressing any commingling of such passengers
and property with passengers and property screened
under the pilot program described in subsection (b);
and

(4) insider risk at foreign last point of depa-
ture airports.

(d) Re-screening of Checked Baggage.—Sub-
ject to subsection (f), the Administrator may determine
whether checked baggage arriving from participating for-
egn airports referenced in subsection (b) that screen
using an explosives detection system must be re-screened
in the United States by an explosives detection system be-
fore such baggage continues on any additional flight or
flight segment.

(e) Aviation Security Screening Agreement.—
An aviation security screening agreement described in this
subsection is a treaty, executive agreement, or other inter-
national arrangement that—

(1)(A) in the case of a treaty or executive
agreement, is signed by the President; and

(B) in the case of an international agreement,
is signed by only the President, Secretary of Home-
land Security, or Administrator, without delegating
such authority; and
(2) is entered into with a foreign country that delineates and implements security standards and protocols utilized at a foreign last point of departure airport that are determined by the Administrator—

(A) to be comparable to those of the United States; and

(B) sufficiently effective to enable passengers and their accessible property to deplane into sterile areas of airports in the United States without the need for re-screening.

(f) RE-SCREENING REQUIREMENT.—

(1) IN GENERAL.—If the Administrator determines that a foreign country participating in the aviation security screening agreement has not maintained and implemented security standards and protocols comparable to those of the United States at foreign last point of departure airports at which a pilot program has been established in accordance with this section, the Administrator shall ensure that passengers and their property arriving from such airports are re-screened in the United States, including by using explosives detection systems in accordance with section 44901(d)(1) of title 49, United States Code, and implementing regulations and directives, before such passengers and their property
are permitted into sterile areas of airports in the United States.

(2) CONSULTATION.—If the Administrator has reasonable grounds to believe that the other party to an aviation security screening agreement has not complied with such agreement, the Administrator shall request immediate consultation with such party.

(3) SUSPENSION OR TERMINATION OF AGREEMENT.—If a satisfactory resolution between TSA and a foreign country is not reached within 45 days after a consultation request under paragraph (2) or in the case of the foreign country’s continued or egregious failure to maintain the security standards and protocols described in paragraph (1), the President, Secretary of Homeland Security, or Administrator, as appropriate, shall suspend or terminate the aviation security screening agreement with such country, as determined appropriate by the President, Secretary of Homeland Security, or Administrator. The Administrator shall notify the appropriate congressional committees of such consultation and suspension or termination, as the case may be, not later than seven days after such consultation and suspension or termination.
(g) Briefings to Congress.—Not later than 45 days before an aviation security screening agreement described in subsection (e) enters into force, the Administrator shall submit to the appropriate congressional committees—

(1) an aviation security threat assessment for the country in which such foreign last point of departure airport is located;

(2) information regarding any corresponding mitigation efforts to address any security issues identified in such threat assessment, including any plans for joint covert testing;

(3) information on potential security vulnerabilities associated with commencing a pilot program at such foreign last point of departure airport pursuant to subsection (b) and mitigation plans to address such potential security vulnerabilities;

(4) an assessment of the impacts such pilot program will have on aviation security;

(5) an assessment of the screening performed at such foreign last point of departure airport, including the feasibility of TSA personnel monitoring screening, security protocols, and standards;

(6) information regarding identifying the entity or entities responsible for screening passengers and
property at such foreign last point of departure airport;

(7) the name of the entity or local authority and any contractor or subcontractor;

(8) information regarding the screening requirements relating to such aviation security screening agreement;

(9) details regarding information sharing mechanisms between the TSA and such foreign last point of departure airport, screening authority, or entity responsible for screening provided for under such aviation security screening agreement; and

(10) a copy of the aviation security screening agreement, which shall identify the foreign last point of departure airport or airports at which a pilot program under this section is to be established.

(h) Certifications Relating to the Pilot Program for One-Stop Security.—For each aviation security screening agreement described in subsection (e), the Administrator shall submit to the appropriate congressional committees—

(1)(A) a certification that such agreement satisfies all of the requirements specified in subsection (c); or
(B) in the event that one or more of such requirements are not so satisfied, a description of the unsatisfied requirement and information on what actions the Administrator will take to ensure that such remaining requirements are satisfied before such agreement enters into force;

(2) a certification that TSA and U.S. Customs and Border Protection have ensured that any necessary physical modifications or appropriate mitigations exist in the domestic one-stop security pilot program airport prior to receiving international passengers from a last point of departure airport under the aviation security screening agreement;

(3) a certification that a foreign last point of departure airport covered by an aviation security screening agreement has an operation to screen all checked bags as required by law, regulation, or international agreement, including the full utilization of explosives detection systems to the extent applicable; and

(4) a certification that the Administrator consulted with stakeholders, including air carriers, aviation nonprofit labor organizations, airport operators, relevant interagency partners, and other stake-
holders that the Administrator determines appropriate.

(i) REPORT TO CONGRESS.—Not later than five years after the date of the enactment of this Act, the Secretary of Homeland Security, in coordination with the Administrator, shall submit a report to the appropriate congressional committees regarding the implementation of the pilot program authorized under this section, including information relating to—

(1) the impact of such program on homeland security and international aviation security, including any benefits and challenges of such program;

(2) the impact of such program on passengers, airports, and air carriers, including any benefits and challenges of such program; and

(3) the impact and feasibility of continuing such program or expanding it into a more permanent program, including any benefits and challenges of such continuation or expansion.

(j) RULE OF CONSTRUCTION.—Nothing in this section may be construed as limiting the authority of U.S. Customs and Border Protection to inspect persons and baggage arriving in the United States in accordance with applicable law.
(k) Sunset.—The pilot program authorized under this section shall terminate on the date that is six years after the date of the enactment of this Act.

SEC. 59140. DHS ILLICIT CROSS-BORDER TUNNEL DEFENSE.

(a) Counter Illicit Cross-border Tunnel Operations Strategic Plan.—

(1) In general.—Not later than 180 days after the date of the enactment of this Act, the Commissioner of U.S. Customs and Border Protection, in coordination with the Under Secretary for Science and Technology, and, as appropriate, other officials of the Department of Homeland Security, shall develop a counter illicit cross-border tunnel operations strategic plan (in this section referred to as the “strategic plan”) to address the following:

(A) Risk-based criteria to be used to prioritize the identification, breach, assessment, and remediation of illicit cross-border tunnels.

(B) Promote the use of innovative technologies to identify, breach, assess, and remediate illicit cross-border tunnels in a manner that, among other considerations, reduces the impact of such activities on surrounding communities.
(C) Processes to share relevant illicit cross-border tunnel location, operations, and technical information.

(D) Indicators of specific types of illicit cross-border tunnels found in each U.S. Border Patrol sector identified through operations to be periodically disseminated to U.S. Border Patrol sector chiefs to educate field personnel.

(E) A counter illicit cross-border tunnel operations resource needs assessment that includes consideration of the following:

(i) Technology needs.

(ii) Staffing needs, including the following:

(I) A position description for counter illicit cross-border tunnel operations personnel.

(II) Any specialized skills required of such personnel.

(III) The number of such full time personnel, disaggregated by U.S. Border Patrol sector.

(2) REPORT TO CONGRESS ON STRATEGIC PLAN.—Not later than one year after the development of the strategic plan, the Commissioner of U.S.
Customs and Border Protection shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the implementation of the strategic plan.

(b) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to the Commissioner of U.S. Customs and Border Protection $1,000,000 for each of fiscal years 2023 and 2024 to carry out—

  (1) the development of the strategic plan; and

  (2) remediation operations of illicit cross-border tunnels in accordance with the strategic plan to the maximum extent practicable.

SEC. 59141. PREVENT EXPOSURE TO NARCOTICS AND TOXICS.

(a) TRAINING FOR U.S. CUSTOMS AND BORDER PROTECTION PERSONNEL ON THE USE OF CONTAINMENT DEVICES TO PREVENT SECONDARY EXPOSURE TO FENTANYL AND OTHER POTENTIALLY LETHAL SUBSTANCES.—Paragraph (1) of section 416(b) of the Homeland Security Act of 2002 (6 U.S.C. 216(b)) is amended by adding at the end the following new subparagraph:

“(C) How to use containment devices to prevent secondary exposure to fentanyl and other potentially lethal substances.”.
(b) AVAILABILITY OF CONTAINMENT DEVICES.—Section 416(c) of the Homeland Security Act of 2002 (6 U.S.C. 216(c)) is amended—

(1) by striking “and” after “equipment” and inserting a comma; and

(2) by inserting “and containment devices” after “naloxone,”.

Subtitle D—Technical, Conforming, and Clerical Amendments

SEC. 59151. TECHNICAL, CONFORMING, AND CLERICAL AMENDMENTS.

The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by—

(1) amending the items relating to sections 435 and 436 to read as follows:

“Sec. 435. Maritime operations coordination plan. 
“Sec. 436. Maritime security capabilities assessments.”;

(2) amending the item relating to section 1617 to read as follows:

“Sec. 1617. Diversified security technology industry marketplace.”;

(3) amending the item relating to section 1621 to read as follows:

“Sec. 1621. Maintenance validation and oversight.”; and

(4) amending the item relating to section 2103 to read as follows:

“Sec. 2103. Protection and sharing of information.”.