114TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPORT
114–756

CYBER PREPAREDNESS ACT OF 2016

SEPTEMBER 19, 2016.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

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

R E P O R T

[To accompany H.R. 5459]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security, to whom was referred the bill (H.R. 5459) to amend the Homeland Security Act of 2002 to enhance preparedness and response capabilities for cyber attacks, bolster the dissemination of homeland security information related to cyber threats, and for other purposes, having considered the same, reports favorably thereon with an amendment and recommends that the bill as amended do pass.

CONTENTS

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Cyber Preparedness Act of 2016".

SEC. 2. INFORMATION SHARING.

Title II of the Homeland Security Act of 2002 is amended—

(1) in section 210A (6 U.S.C. 124h)—

(A) in subsection (b)—

(i) in paragraph (10), by inserting before the semicolon at the end the following: ", including, in coordination with the national cybersecurity and communications integration center under section 227, accessing timely technical assistance, risk management support, and incident response capabilities with respect to cyber threat indicators, defensive measures, cybersecurity risks, and incidents (as such terms are defined in such section), which may include attribution, mitigation, and remediation, and the provision of information and recommendations on security and resilience, including implications of cybersecurity risks to equipment and technology related to the electoral process";

(ii) in paragraph (11), by striking "and" after the semicolon;

(iii) by redesignating paragraph (12) as paragraph (14); and

(iv) by inserting after paragraph (11) the following new paragraphs:

"(12) review information relating to cybersecurity risks that is gathered by State, local, and regional fusion centers, and incorporate such information, as appropriate, into the Department's own information relating to cybersecurity risks;

"(13) ensure the dissemination to State, local, and regional fusion centers of information relating to cybersecurity risks; and";

(B) in subsection (c)(2)—

(i) by redesignating subparagraphs (C) through (G) as subparagraphs (D) through (H), respectively; and

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

"(C) The national cybersecurity and communications integration center under section 227.";

(C) in subsection (d)—

(i) in paragraph (3), by striking "and" after the semicolon;

(ii) by redesignating paragraph (4) as paragraph (5); and

(iii) by inserting after paragraph (3) the following new paragraph:

"(4) assist, in coordination with the national cybersecurity and communications integration center under section 227, fusion centers in using information relating to cybersecurity risks to develop a comprehensive and accurate threat picture; and"; and

(D) in subsection (j)—

(i) by redesignating paragraphs (1) through (5) as paragraphs (2) through (6), respectively; and

(ii) by inserting before paragraph (2), as so redesignated, the following new paragraph:

"(1) the term 'cybersecurity risk' has the meaning given that term in section 227;"; and

(2) in section 227 (6 U.S.C. 148)—

(A) in subsection (c)—

(i) in paragraph (5)(B), by inserting ", including State and major urban area fusion centers, as appropriate" before the semicolon at the end;

(ii) in paragraph (7), in the matter preceding subparagraph (A), by striking "information and recommendations" each place it appears and inserting "information, recommendations, and best practices"; and

(iii) in paragraph (9), by inserting "and best practices" after "defensive measures"; and

(B) in subsection (d)(1)(B)(ii), by inserting "and State and major urban area fusion centers, as appropriate" before the semicolon at the end.

SEC. 3. HOMELAND SECURITY GRANTS.

Subsection (a) of section 2008 of the Homeland Security Act of 2002 (6 U.S.C. 609) is amended—

(1) by redesignating paragraphs (4) through (14) as paragraphs (5) through (15), respectively; and

(2) by inserting after paragraph (3) the following new paragraph:

"(4) enhancing cybersecurity, including preparing for and responding to cybersecurity risks and incidents and developing State-wide cyber threat information analysis and dissemination activities;".

SEC. 4. SENSE OF CONGRESS.

It is the sense of Congress that to facilitate the timely dissemination to appropriate State, local, and private sector stakeholders of homeland security information related to cyber threats, the Secretary of Homeland Security should, to the greatest extent practicable, work to share actionable information related to cyber threats in an unclassified form.

PURPOSE AND SUMMARY

The purpose of H.R. 5459 is to amend the Homeland Security Act of 2002 to enhance preparedness and response capabilities for cyber attacks, bolster the dissemination of homeland security information related to cyber threats, and for other purposes.

BACKGROUND AND NEED FOR LEGISLATION

Cybersecurity is a major national security issue and the threat is real and immediate. For instance, a cyber-attack causing widespread power outages could have major cascading consequences on public health and safety.

During a joint hearing of the Subcommittees on Emergency Preparedness, Response, and Communications and Cybersecurity, Infrastructure Protection, and Security Technologies on May 24, 2016, Members heard from State officials about their best practices and lessons learned in enhancing cybersecurity capabilities and how the Federal Government can help mitigate some of the challenges States face.

Among the issues raised by the witnesses was the need for better information sharing between the National Cybersecurity and Communications Integration Center (NCCIC) and state and major urban area fusion centers; the need for clarity on the use of homeland security grants to address cybersecurity; and the impact the level of classification of cyber threat information has on States and fusion centers' ability to share that information with relevant stakeholders. This legislation seeks to address these concerns.

HEARINGS

The Committee did not hold any legislative hearings on H.R. 5459. However, the Subcommittee on Emergency Preparedness, Response, and Communications and the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies held a joint hearing on May 24, 2016, entitled "Enhancing Preparedness and Response Capabilities to Address Cyber Threats." The Subcommittees received testimony from Mr. Mark Ghilarducci, Director, Emergency Services, Office of the Governor, State of California; Lt. Col. Daniel J. Cooney, Assistant Deputy Superintendent, Office of Counter Terrorism, New York State Police; Brig. Gen. Steven Spano (Ret.—USAF), President and Chief Operating Officer, Center for Internet Security; Mr. Mark Raymond, Vice President, National Association of State Chief Information Officers; and Mr. Robert Galvin, Chief Technology Officer, Port Authority of New York and New Jersey.

The testimony received provided the basis for H.R. 5459.

COMMITTEE CONSIDERATION

The Committee met on September 13, 2016, to consider H.R. 5459, and ordered the measure to be reported to the House with

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

The following amendments were offered:

An Amendment in the Nature of a Substitute offered by MR. DONOVAN (#1); was AGREED TO, as amended, by voice vote.

An amendment by MR. THOMPSON of Mississippi to the Amendment in the Nature of a Substitute (#1A); was AGREED TO by voice vote.

Page 1, line 9, insert the following (and make necessary conforming changes):
(i) in paragraph (10), by inserting before the semicolon at the end the following: ", including, in coordination with the national cybersecurity and communications integration center under section 227, accessing timely technical assistance, risk management support, and incident response capabilities with respect to cyber threat indicators, defensive measures, cybersecurity risks, and incidents (as such terms are defined in such section), which may include attribution, mitigation, and remediation, and the provision of information and recommendations on security and resilience, including implications of cybersecurity risks to equipment and technology related to the electoral process".

An amendment by MR. LANGEVIN to the Amendment in the Nature of a Substitute (#1B); was AGREED TO by voice vote.

Page 2, line 6, inset the following (and make necessary conforming changes):
(B) in subsection (c)(2)—
(i) by redesignating subparagraphs (C) through (G) as subparagraphs (D) through (H), respectively; and
(ii) by inserting after subparagraph (B) the follow new subparagraph:
"(C) The national cybersecurity and communications integration center under section 227."

An amendment by MS. LORETTA SANCHEZ of California to the Amendment in the Nature of a Substitute (#1C); was AGREED TO by voice vote.

Page 4, line 8, insert "and developing State-wide cyber threat information analysis and dissemination activities" after "incidents".

The Subcommittee on Emergency Preparedness, Response, and Communications met on June 16, 2016, to consider H.R. 5459, and ordered the measure reported to the Full Committee with a favorable recommendation, without amendment, by voice vote.

COMMITTEE VOTES

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

No recorded votes were requested during consideration of H.R. 5459.

COMMITTEE OVERSIGHT FINDINGS

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

NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

In compliance with clause 3(c)(2) of Rule XIII of the Rules of the House of Representatives, the Committee finds that H.R. 5459, the Cyber Preparedness Act of 2016, would result in no new or increased budget authority, entitlement authority, or tax expenditures or revenues.

CONGRESSIONAL BUDGET OFFICE ESTIMATE

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

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, September 16, 2016.

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

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 5459, the Cyber Preparedness Act of 2016.

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

Sincerely,

MARK P. HADLEY
(for Keith Hall, *Director*).

Enclosure.

H.R. 5459—Cyber Preparedness Act of 2016

H.R. 5459 would amend the Homeland Security Act of 2002 to require the Department of Homeland Security (DHS) to provide cybersecurity assistance to, and share cybersecurity risk information with, state, local, and regional fusion centers. Fusion centers are collaborative efforts among federal, state, local, or tribal government agencies that combine resources, expertise, or information related to criminal or terrorist activity. The bill also would expand membership of the National Cybersecurity and Communications Integration Center to include state and fusion centers in major urban areas. Under current law, DHS currently provides cybersecurity assistance to, and shares cybersecurity risk information with, fusion centers; the bill would codify those efforts.

The bill also would authorize recipients of Urban Area Initiative or State Homeland Security grants to use those funds to enhance cybersecurity at the state, local, or tribal government levels. The bill would not alter the number or dollar amount of grants provided or the eligibility requirements for receiving those grants.

CBO estimates that implementing H.R. 5459 would have no significant effect on the federal budget over the 2017–2021 period.

Enacting H.R. 5459 would not affect direct spending or revenues; therefore, pay-as-you-go procedures do not apply. CBO estimates that enacting H.R. 5459 would not increase net direct spending or on-budget deficits in any of the four consecutive 10-year periods beginning in 2027.

H.R. 5459 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act. State, local, and tribal governments receiving Urban Area Initiative or State Homeland Security grants would benefit from the ability to use such funds to prepare and respond to cybersecurity risks and incidents. Any costs to state, local, or tribal governments, including matching contributions, would result from complying with conditions of assistance.

The CBO staff contacts for this estimate are Robert Reese and Bill Ma (for federal costs) and Rachel Austin (for intergovernmental effects). The estimate was approved by H. Samuel Papenfuss, Deputy Assistant Director for Budget Analysis.

STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause 3(c)(4) of Rule XIII of the Rules of the House of Representatives, H.R. 5459 contains the following general performance goals and objectives, including outcome related goals and objectives authorized.

The goal of H.R. 5459 is to enhance preparedness and response capabilities for cyber attacks and bolster the sharing of information related to cyber threats, to allow cyber preparedness activities as an allowable use of State Homeland Security Grant Program and the Urban Area Security Initiative funding, and to encourage the Department of Homeland Security to work on creating tear lines for cyber threat and risk information.

DUPLICATIVE FEDERAL PROGRAMS

Pursuant to clause 3(c) of Rule XIII, the Committee finds that H.R. 5459 does not contain any provision that establishes or reauthorizes a program known to be duplicative of another Federal program.

CONGRESSIONAL EARMARKS, LIMITED TAX BENEFITS, AND LIMITED TARIFF BENEFITS

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

FEDERAL MANDATES STATEMENT

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

PREEMPTION CLARIFICATION

In compliance with section 423 of the Congressional Budget Act of 1974, requiring the report of any Committee on a bill or joint resolution to include a statement on the extent to which the bill or joint resolution is intended to preempt State, local, or Tribal law, the Committee finds that H.R. 5459 does not preempt any State, local, or Tribal law.

DISCLOSURE OF DIRECTED RULE MAKINGS

The Committee estimates that H.R. 5459 would require no directed rule makings.

ADVISORY COMMITTEE STATEMENT

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

APPLICABILITY TO LEGISLATIVE BRANCH

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

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short Title.

This section provides that this bill may be cited as the "Cyber Preparedness Act of 2016".

Sec. 2. Information Sharing.

In an effort to address issues with cyber information sharing raised by witnesses at the May 24th joint hearing of the Subcommittees on Emergency Preparedness, Response, and Communications and Cybersecurity, Infrastructure Protection, and Security Technologies, this section seeks to ensure information related to cyber risks and threats is shared with state and major urban area fusion centers (fusion centers). Additionally, this section includes, as a function of the NCCIC, sharing information about cyber best practices, in addition to the sharing of cyber threat indicators and defensive measures currently required by law. Lastly, this section authorizes representatives from State and major urban area fusion centers to be assigned to the NCCIC, similar to the assignment of representatives from information sharing and analysis centers (ISACs) permitted under current law and permits NCCIC personnel to be deployed to fusion centers.

The Committee has heard that, while improving, the flow of federal cyber threat and risk information to state and local emergency services providers is slow and overclassified. The current process of sharing information usually causes emergency services providers to be reactive rather than proactive in addressing the current cyber threats. To date, there are 78 fusion centers across the Nation with the primary mission to serve as the conduit between the Federal Government and States and localities for the sharing of intelligence and homeland security information. Most fusion centers have developed dissemination channels that can be used to ensure cyber threat and risk information is getting to the appropriate emergency response providers. Additionally, the Committee supports an increase in coordination between NCCIC and fusion centers. This section will ensure the coordination efforts continue by allowing representatives from the National Network of Fusion Centers to physically sit at the NCCIC and NCCIC personnel to be assigned to fusion centers.

Lastly, the Committee has learned that many States have proactively taken steps to improve their cybersecurity posture. These best practices should to be shared in a formal way with other States and entities to continue building and enhancing the Nation's cybersecurity capabilities.

Sec. 3. Homeland Security Grants.

This section authorizes the use of State Homeland Security Grant Program (SHSGP) and Urban Area Security Initiative

(UASI) funds for cybersecurity enhancements. While States and urban areas are currently permitted to use SHSGP and UASI funds to increase their cybersecurity posture, this section will codify that cyber preparedness activities are allowable uses for both grant programs. For several years now, FEMA has released an annual National Preparedness Report, which highlights the States' 32 preparedness core capabilities, as defined by the National Preparedness Goal. Since the first National Preparedness Report was released in 2012, States have ranked their cybersecurity capabilities as one of their lowest. The Committee believes the ability for States and urban areas to use SHSGP and UASI funds for cyber preparedness is essential and this section will ensure that SHSGP and USAI funds remain available for cyber preparedness.

Sec. 4. Sense of Congress.

This section expresses the sense of Congress that the Department of Homeland Security should, to the greatest extent practicable, work to establish tear lines so actionable intelligence related to cyber threats may be shared with those without clearances. The Committee has heard from emergency response providers, time and time again, that cyber threat information is overclassified which prohibits their ability to receive and disseminate cyber threat information. The majority of emergency response providers are not cleared to the TS//SCI or even the Top Secret level. The Committee believes the Department should work on establishing tear lines to ensure valuable cyber threat information is disseminated to all appropriate stakeholders.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

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

HOMELAND SECURITY ACT OF 2002

* * * * * * *

TITLE II—INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION

* * * * * * *

Subtitle A—Information and Analysis and Infrastructure Protection; Access to Information

* * * * * * *

SEC. 210A. DEPARTMENT OF HOMELAND SECURITY STATE, LOCAL, AND REGIONAL FUSION CENTER INITIATIVE.

(a) ESTABLISHMENT.—The Secretary, in consultation with the program manager of the information sharing environment established under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485), the Attorney General, the Privacy Officer of the Department, the Officer for Civil Rights and Civil Liberties of the Department, and the Privacy and Civil Liberties Oversight Board established under section 1061 of the Intelligence Reform and Terrorism Prevention Act of 2004 (5 U.S.C. 601 note), shall establish a Department of Homeland Security State, Local, and Regional Fusion Center Initiative to establish partnerships with State, local, and regional fusion centers.

(b) DEPARTMENT SUPPORT AND COORDINATION.—Through the Department of Homeland Security State, Local, and Regional Fusion Center Initiative, and in coordination with the principal officials of participating State, local, or regional fusion centers and the officers designated as the Homeland Security Advisors of the States, the Secretary shall—

(1) provide operational and intelligence advice and assistance to State, local, and regional fusion centers;

(2) support efforts to include State, local, and regional fusion centers into efforts to establish an information sharing environment;

(3) conduct tabletop and live training exercises to regularly assess the capability of individual and regional networks of State, local, and regional fusion centers to integrate the efforts of such networks with the efforts of the Department;

(4) coordinate with other relevant Federal entities engaged in homeland security-related activities;

(5) provide analytic and reporting advice and assistance to State, local, and regional fusion centers;

(6) review information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, that is gathered by State, local, and regional fusion centers, and to incorporate such information, as appropriate, into the Department's own such information;

(7) provide management assistance to State, local, and regional fusion centers;

(8) serve as a point of contact to ensure the dissemination of information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information;

(9) facilitate close communication and coordination between State, local, and regional fusion centers and the Department;

(10) provide State, local, and regional fusion centers with expertise on Department resources and operations*, including, in coordination with the national cybersecurity and communications integration center under section 227, accessing timely technical assistance, risk management support, and incident response capabilities with respect to cyber threat indicators, defensive measures, cybersecurity risks, and incidents (as such terms are defined in such section), which may include attribution, mitigation, and remediation, and the provision of informa-*

tion and recommendations on security and resilience, including implications of cybersecurity risks to equipment and technology related to the electoral process;

(11) provide training to State, local, and regional fusion centers and encourage such fusion centers to participate in terrorism threat-related exercises conducted by the Department; [and]

(12) review information relating to cybersecurity risks that is gathered by State, local, and regional fusion centers, and incorporate such information, as appropriate, into the Department's own information relating to cybersecurity risks;

(13) ensure the dissemination to State, local, and regional fusion centers of information relating to cybersecurity risks; and

[(12)] *(14)* carry out such other duties as the Secretary determines are appropriate.

(c) PERSONNEL ASSIGNMENT.—

(1) IN GENERAL.—The Under Secretary for Intelligence and Analysis shall, to the maximum extent practicable, assign officers and intelligence analysts from components of the Department to participating State, local, and regional fusion centers.

(2) PERSONNEL SOURCES.—Officers and intelligence analysts assigned to participating fusion centers under this subsection may be assigned from the following Department components, in coordination with the respective component head and in consultation with the principal officials of participating fusion centers:

(A) Office of Intelligence and Analysis.

(B) Office of Infrastructure Protection.

(C) The national cybersecurity and communications integration center under section 227.

[(C)] *(D)* Transportation Security Administration.

[(D)] *(E)* United States Customs and Border Protection.

[(E)] *(F)* United States Immigration and Customs Enforcement.

[(F)] *(G)* United States Coast Guard.

[(G)] *(H)* Other components of the Department, as determined by the Secretary.

(3) QUALIFYING CRITERIA.—

(A) IN GENERAL.—The Secretary shall develop qualifying criteria for a fusion center to participate in the assigning of Department officers or intelligence analysts under this section.

(B) CRITERIA.—Any criteria developed under subparagraph (A) may include—

(i) whether the fusion center, through its mission and governance structure, focuses on a broad counterterrorism approach, and whether that broad approach is pervasive through all levels of the organization;

(ii) whether the fusion center has sufficient numbers of adequately trained personnel to support a broad counterterrorism mission;

(iii) whether the fusion center has—

(I) access to relevant law enforcement, emergency response, private sector, open source, and national security data; and

(II) the ability to share and analytically utilize that data for lawful purposes;

(iv) whether the fusion center is adequately funded by the State, local, or regional government to support its counterterrorism mission; and

(v) the relevancy of the mission of the fusion center to the particular source component of Department officers or intelligence analysts.

(4) PREREQUISITE.—

(A) INTELLIGENCE ANALYSIS, PRIVACY, AND CIVIL LIBERTIES TRAINING.—Before being assigned to a fusion center under this section, an officer or intelligence analyst shall undergo—

(i) appropriate intelligence analysis or information sharing training using an intelligence-led policing curriculum that is consistent with—

(I) standard training and education programs offered to Department law enforcement and intelligence personnel; and

(II) the Criminal Intelligence Systems Operating Policies under part 23 of title 28, Code of Federal Regulations (or any corresponding similar rule or regulation);

(ii) appropriate privacy and civil liberties training that is developed, supported, or sponsored by the Privacy Officer appointed under section 222 and the Officer for Civil Rights and Civil Liberties of the Department, in consultation with the Privacy and Civil Liberties Oversight Board established under section 1061 of the Intelligence Reform and Terrorism Prevention Act of 2004 (5 U.S.C. 601 note); and

(iii) such other training prescribed by the Under Secretary for Intelligence and Analysis.

(B) PRIOR WORK EXPERIENCE IN AREA.—In determining the eligibility of an officer or intelligence analyst to be assigned to a fusion center under this section, the Under Secretary for Intelligence and Analysis shall consider the familiarity of the officer or intelligence analyst with the State, locality, or region, as determined by such factors as whether the officer or intelligence analyst—

(i) has been previously assigned in the geographic area; or

(ii) has previously worked with intelligence officials or law enforcement or other emergency response providers from that State, locality, or region.

(5) EXPEDITED SECURITY CLEARANCE PROCESSING.—The Under Secretary for Intelligence and Analysis—

(A) shall ensure that each officer or intelligence analyst assigned to a fusion center under this section has the appropriate security clearance to contribute effectively to the mission of the fusion center; and

(B) may request that security clearance processing be expedited for each such officer or intelligence analyst and may use available funds for such purpose.

(6) FURTHER QUALIFICATIONS.—Each officer or intelligence analyst assigned to a fusion center under this section shall satisfy any other qualifications the Under Secretary for Intelligence and Analysis may prescribe.

(d) RESPONSIBILITIES.—An officer or intelligence analyst assigned to a fusion center under this section shall—

(1) assist law enforcement agencies and other emergency response providers of State, local, and tribal governments and fusion center personnel in using information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, to develop a comprehensive and accurate threat picture;

(2) review homeland security-relevant information from law enforcement agencies and other emergency response providers of State, local, and tribal government;

(3) create intelligence and other information products derived from such information and other homeland security-relevant information provided by the Department; [and]

(4) assist, in coordination with the national cybersecurity and communications integration center under section 227, fusion centers in using information relating to cybersecurity risks to develop a comprehensive and accurate threat picture; and

[(4)] *(5)* assist in the dissemination of such products, as coordinated by the Under Secretary for Intelligence and Analysis, to law enforcement agencies and other emergency response providers of State, local, and tribal government, other fusion centers, and appropriate Federal agencies.

(e) BORDER INTELLIGENCE PRIORITY.—

(1) IN GENERAL.—The Secretary shall make it a priority to assign officers and intelligence analysts under this section from United States Customs and Border Protection, United States Immigration and Customs Enforcement, and the Coast Guard to participating State, local, and regional fusion centers located in jurisdictions along land or maritime borders of the United States in order to enhance the integrity of and security at such borders by helping Federal, State, local, and tribal law enforcement authorities to identify, investigate, and otherwise interdict persons, weapons, and related contraband that pose a threat to homeland security.

(2) BORDER INTELLIGENCE PRODUCTS.—When performing the responsibilities described in subsection (d), officers and intelligence analysts assigned to participating State, local, and regional fusion centers under this section shall have, as a primary responsibility, the creation of border intelligence products that—

(A) assist State, local, and tribal law enforcement agencies in deploying their resources most efficiently to help detect and interdict terrorists, weapons of mass destruction, and related contraband at land or maritime borders of the United States;

(B) promote more consistent and timely sharing of border security-relevant information among jurisdictions along land or maritime borders of the United States; and

(C) enhance the Department's situational awareness of the threat of acts of terrorism at or involving the land or maritime borders of the United States.

(f) DATABASE ACCESS.—In order to fulfill the objectives described under subsection (d), each officer or intelligence analyst assigned to a fusion center under this section shall have appropriate access to all relevant Federal databases and information systems, consistent with any policies, guidelines, procedures, instructions, or standards established by the President or, as appropriate, the program manager of the information sharing environment for the implementation and management of that environment.

(g) CONSUMER FEEDBACK.—

(1) IN GENERAL.—The Secretary shall create a voluntary mechanism for any State, local, or tribal law enforcement officer or other emergency response provider who is a consumer of the intelligence or other information products referred to in subsection (d) to provide feedback to the Department on the quality and utility of such intelligence products.

(2) REPORT.—Not later than one year after the date of the enactment of the Implementing Recommendations of the 9/11 Commission Act of 2007, and annually thereafter, the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report that includes a description of the consumer feedback obtained under paragraph (1) and, if applicable, how the Department has adjusted its production of intelligence products in response to that consumer feedback.

(h) RULE OF CONSTRUCTION.—

(1) IN GENERAL.—The authorities granted under this section shall supplement the authorities granted under section 201(d) and nothing in this section shall be construed to abrogate the authorities granted under section 201(d).

(2) PARTICIPATION.—Nothing in this section shall be construed to require a State, local, or regional government or entity to accept the assignment of officers or intelligence analysts of the Department into the fusion center of that State, locality, or region.

(i) GUIDELINES.—The Secretary, in consultation with the Attorney General, shall establish guidelines for fusion centers created and operated by State and local governments, to include standards that any such fusion center shall—

(1) collaboratively develop a mission statement, identify expectations and goals, measure performance, and determine effectiveness for that fusion center;

(2) create a representative governance structure that includes law enforcement officers and other emergency response providers and, as appropriate, the private sector;

(3) create a collaborative environment for the sharing of intelligence and information among Federal, State, local, and tribal government agencies (including law enforcement officers and other emergency response providers), the private sector, and the public, consistent with any policies, guidelines, procedures, instructions, or standards established by the President

or, as appropriate, the program manager of the information sharing environment;

(4) leverage the databases, systems, and networks available from public and private sector entities, in accordance with all applicable laws, to maximize information sharing;

(5) develop, publish, and adhere to a privacy and civil liberties policy consistent with Federal, State, and local law;

(6) provide, in coordination with the Privacy Officer of the Department and the Officer for Civil Rights and Civil Liberties of the Department, appropriate privacy and civil liberties training for all State, local, tribal, and private sector representatives at the fusion center;

(7) ensure appropriate security measures are in place for the facility, data, and personnel;

(8) select and train personnel based on the needs, mission, goals, and functions of that fusion center;

(9) offer a variety of intelligence and information services and products to recipients of fusion center intelligence and information; and

(10) incorporate law enforcement officers, other emergency response providers, and, as appropriate, the private sector, into all relevant phases of the intelligence and fusion process, consistent with the mission statement developed under paragraph (1), either through full time representatives or liaison relationships with the fusion center to enable the receipt and sharing of information and intelligence.

(j) DEFINITIONS.—In this section—

(1) the term "cybersecurity risk" has the meaning given that term in section 227;

[(1)**]** *(2)* the term "fusion center" means a collaborative effort of 2 or more Federal, State, local, or tribal government agencies that combines resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal or terrorist activity;

[(2)**]** *(3)* the term "information sharing environment" means the information sharing environment established under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485);

[(3)**]** *(4)* the term "intelligence analyst" means an individual who regularly advises, administers, supervises, or performs work in the collection, gathering, analysis, evaluation, reporting, production, or dissemination of information on political, economic, social, cultural, physical, geographical, scientific, or military conditions, trends, or forces in foreign or domestic areas that directly or indirectly affect national security;

[(4)**]** *(5)* the term "intelligence-led policing" means the collection and analysis of information to produce an intelligence end product designed to inform law enforcement decision making at the tactical and strategic levels; and

[(5)**]** *(6)* the term "terrorism information" has the meaning given that term in section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485).

(k) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated $10,000,000 for each of fiscal years 2008 through

2012, to carry out this section, except for subsection (i), including for hiring officers and intelligence analysts to replace officers and intelligence analysts who are assigned to fusion centers under this section.

* * * * * * *

Subtitle C—Information Security

* * * * * * *

SEC. 227. NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER.

(a) DEFINITIONS.—In this section—

(1) the term "cybersecurity risk"—

(A) means threats to and vulnerabilities of information or information systems and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of such information or information systems, including such related consequences caused by an act of terrorism; and

(B) does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement;

(2) the terms "cyber threat indicator" and "defensive measure" have the meanings given those terms in section 102 of the Cybersecurity Act of 2015;

(3) the term "incident" means an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system;

(4) the term "information sharing and analysis organization" has the meaning given that term in section 212(5);

(5) the term "information system" has the meaning given that term in section 3502(8) of title 44, United States Code; and

(6) the term "sharing" (including all conjugations thereof) means providing, receiving, and disseminating (including all conjugations of each of such terms).

(b) CENTER.—There is in the Department a national cybersecurity and communications integration center (referred to in this section as the "Center") to carry out certain responsibilities of the Under Secretary appointed under section 103(a)(1)(H).

(c) FUNCTIONS.—The cybersecurity functions of the Center shall include—

(1) being a Federal civilian interface for the multi-directional and cross-sector sharing of information related to cyber threat indicators, defensivemeasures, cybersecurity risks, incidents, analysis, and warnings for Federal and non-Federal entities, including the implementationof title I of the Cybersecurity Act of 2015;

(2) providing shared situational awareness to enable real-time, integrated, and operational actions across the Federal

Government and non-Federal entities to address cybersecurity risks and incidents to Federal and non-Federal entities;

(3) coordinating the sharing of information related to cyber threat indicators, defensive measures,cybersecurity risks, and incidents across the Federal Government;

(4) facilitating cross-sector coordination to address cybersecurity risks and incidents, including cybersecurity risks and incidents that may be related or could have consequential impacts across multiple sectors;

(5)(A) conducting integration and analysis, including cross-sector integration and analysis, of cyber threat indicators, defensivemeasures, cybersecurity risks, and incidents; and

(B) sharing the analysis conducted under subparagraph (A) with Federal and non-Federal entities*, including State and major urban area fusion centers, as appropriate*;

(6) upon request, providing timely technical assistance, risk management support, and incident response capabilities to Federal and non-Federal entities with respect to cyber threat indicators, defensive measures, cybersecurityrisks, and incidents, which may include attribution, mitigation, and remediation;

(7) providing ⟦information and recommendations⟧ *information, recommendations, and best practices* on security and resilience measures to Federal and non-Federal entities, including ⟦information and recommendations⟧ *information, recommendations, and best practices* to—

(A) facilitate information security;

(B) strengthen information systems against cybersecurity risks and incidents; and

(C) sharing cyber threat indicators and defensive measures;

(8) engaging with international partners, in consultation with other appropriate agencies, to—

(A) collaborate on cyber threat indicators, defensive measures, and information related to cybersecurity risks and incidents; and

(B) enhance the security and resilience of global cybersecurity;

(9) sharing cyber threat indicators, defensive measures *and best practices*, and other information related to cybersecurity risks and incidents with Federal and non-Federal entities, including across sectors of critical infrastructure and with State and major urban area fusion centers, as appropriate;

(10) participating, as appropriate, in national exercises run by the Department; and

(11) in coordination with the Office of Emergency Communications of the Department, assessing and evaluating consequence, vulnerability, and threat information regarding cyber incidents to public safety communications to help facilitate continuous improvements to the security and resiliency of such communications.

(d) COMPOSITION.—

(1) IN GENERAL.—The Center shall be composed of—

(A) appropriate representatives of Federal entities, such as—

(i) sector-specific agencies;
(ii) civilian and law enforcement agencies; and
(iii) elements of the intelligence community, as that term is defined under section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4));
(B) appropriate representatives of non-Federal entities, such as—
(i) State, local, and tribal governments;
(ii) information sharing and analysis organizations, including information sharing and analysis centers *and State and major urban area fusion centers, as appropriate*;
(iii) owners and operators of critical information systems; and
(iv) private entities;
(C) components within the Center that carry out cybersecurity and communications activities;
(D) a designated Federal official for operational coordination with and across each sector;
(E) an entity that collaborates with State and local governments on cybersecurity risks and incidents, and has entered into a voluntary information sharing relationship with the Center; and
(F) other appropriate representatives or entities, as determined by the Secretary.
(2) INCIDENTS.—In the event of an incident, during exigent circumstances the Secretary may grant a Federal or non-Federal entity immediate temporary access to the Center.
(e) PRINCIPLES.—In carrying out the functions under subsection (c), the Center shall ensure—
(1) to the extent practicable, that—
(A) timely, actionable, and relevant cyber threatindicators, defensive measures, and information related to cybersecurity risks, incidents, and analysis is shared;
(B) when appropriate, cyber threatindicators, defensive measures, and information related to cybersecurity risks, incidents, and analysis is integrated with other relevant information and tailored to the specific characteristics of a sector;
(C) activities are prioritized and conducted based on the level of risk;
(D) industry sector-specific, academic, and national laboratory expertise is sought and receives appropriate consideration;
(E) continuous, collaborative, and inclusive coordination occurs—
(i) across sectors; and
(ii) with—
(I) sector coordinating councils;
(II) information sharing and analysis organizations; and
(III) other appropriate non-Federal partners;
(F) as appropriate, the Center works to develop and use mechanisms for sharing information related to cyber

threat indicators, defensive measures,cybersecurity risks, and incidents that are technology-neutral, interoperable, real-time, cost-effective, and resilient;

(G) the Center works with other agencies to reduce unnecessarily duplicative sharing of information related to cyber threat indicators,defensive measures, cybersecurity risks, andincidents; and;

(H) the Center designates an agency contact for non-Federal entities;

(2) that information related to cyber threat indicators, defensive measures, cybersecurityrisks, and incidents is appropriately safeguarded against unauthorized access or disclosure; and

(3) that activities conducted by the Center comply with all policies, regulations, and laws that protect the privacy and civil liberties of United States persons, including by working withthe Privacy Officer appointed under section 222 to ensurethat the Center follows the policies and procedures specifiedin subsections (b) and (d)(5)(C) of section 105 of the CybersecurityAct of 2015.

(f) NO RIGHT OR BENEFIT.—

(1) IN GENERAL.—The provision of assistance or information to, and inclusion in the Center of, governmental or private entities under this section shall be at the sole and unreviewable discretion of the Under Secretary appointed under section 103(a)(1)(H).

(2) CERTAIN ASSISTANCE OR INFORMATION.—The provision of certain assistance or information to, or inclusion in the Center of, one governmental or private entity pursuant to this section shall not create a right or benefit, substantive or procedural, to similar assistance or information for any other governmental or private entity.

(g) AUTOMATED INFORMATION SHARING.—

(1) IN GENERAL.—The Under Secretary appointed under section 103(a)(1)(H), in coordination with industry and other stakeholders, shall develop capabilities making use of existing information technology industry standards and best practices, as appropriate, that support and rapidly advance the development, adoption, and implementation of automated mechanisms for the sharing of cyber threat indicators and defensive measures in accordance with title I of the Cybersecurity Act of 2015.

(2) ANNUAL REPORT.—The Under Secretary appointed under section 103(a)(1)(H) 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 an annual report on the status and progress of the development of the capabilities described in paragraph (1). Such reports shall be required until such capabilities are fully implemented.

(h) VOLUNTARY INFORMATION SHARING PROCEDURES.—

(1) PROCEDURES.—

(A) IN GENERAL.—The Center may enter into a voluntary information sharing relationship with any consenting non-Federal entity for the sharing of cyber threat indicators and defensive measures for cybersecurity purposes in ac-

cordance with this section. Nothing in this subsection may be construed to require any non-Federal entity to enter into any such information sharing relationship with the Center or any other entity. The Center may terminate a voluntary information sharing relationship under this subsection, at the sole and unreviewable discretion of the Secretary, acting through the Under Secretary appointed under section 103(a)(1)(H), for any reason, including if the Center determines that the non-Federal entity with which the Center has entered into such a relationship has violated the terms of this subsection.

(B) NATIONAL SECURITY.—The Secretary may decline to enter into a voluntary information sharing relationship under this subsection, at the sole and unreviewable discretion of the Secretary, acting through the Under Secretary appointed under section 103(a)(1)(H), for any reason, including if the Secretary determines that such is appropriate for national security.

(2) VOLUNTARY INFORMATION SHARING RELATIONSHIPS.—A voluntary information sharing relationship under this subsection may be characterized as an agreement described in this paragraph.

(A) STANDARD AGREEMENT.—For the use of a non-Federal entity, the Center shall make available a standard agreement, consistent with this section, on the Department's website.

(B) NEGOTIATED AGREEMENT.—At the request of a non-Federal entity, and if determined appropriate by the Center, at the sole and unreviewable discretion of the Secretary, acting through the Under Secretary appointed under section 103(a)(1)(H), the Department shall negotiate a non-standard agreement, consistent with this section.

(C) EXISTING AGREEMENTS.—An agreement between the Center and a non-Federal entity that is entered into before the date of enactment of this subsection, or such an agreement that is in effect before such date, shall be deemed in compliance with the requirements of this subsection, notwithstanding any other provision or requirement of this subsection. An agreement under this subsection shall include the relevant privacy protections as in effect under the Cooperative Research and Development Agreement for Cybersecurity Information Sharing and Collaboration, as of December 31, 2014. Nothing in this subsection may be construed to require a non-Federal entity to enter into either a standard or negotiated agreement to be in compliance with this subsection.

(i) DIRECT REPORTING.—The Secretary shall develop policies and procedures for direct reporting to the Secretary by the Director of the Center regarding significant cybersecurity risks and incidents.

(j) REPORTS ON INTERNATIONAL COOPERATION.—Not later than 180 days after the date of enactment of this subsection, and periodically thereafter, 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 report on the range of efforts underway

to bolster cybersecurity collaboration with relevant international partners in accordance with subsection (c)(8).

(k) OUTREACH.—Not later than 60 days after the date of enactment of this subsection, the Secretary, acting through the Under Secretary appointed under section 103(a)(1)(H), shall—

(1) disseminate to the public information about how to voluntarily share cyber threat indicators and defensive measures with the Center; and

(2) enhance outreach to critical infrastructure owners and operators for purposes of such sharing.

(l) COORDINATED VULNERABILITY DISCLOSURE.—The Secretary, in coordination with industry and other stakeholders, may develop and adhere to Department policies and procedures for coordinating vulnerability disclosures.

* * * * * * *

TITLE XX—HOMELAND SECURITY GRANTS

* * * * * * *

Subtitle A—Grants to States and High-Risk Urban Areas

* * * * * * *

SEC. 2008. USE OF FUNDS.

(a) PERMITTED USES.—The Administrator shall permit the recipient of a grant under section 2003 or 2004 to use grant funds to achieve target capabilities related to preventing, preparing for, protecting against, and responding to acts of terrorism, consistent with a State homeland security plan and relevant local, tribal, and regional homeland security plans, including by working in conjunction with a National Laboratory (as defined in section 2(3) of the Energy Policy Act of 2005 (42 U.S.C. 15801(3))), through—

(1) developing and enhancing homeland security, emergency management, or other relevant plans, assessments, or mutual aid agreements;

(2) designing, conducting, and evaluating training and exercises, including training and exercises conducted under section 512 of this Act and section 648 of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 748);

(3) protecting a system or asset included on the prioritized critical infrastructure list established under section 210E(a)(2);

(4) enhancing cybersecurity, including preparing for and responding to cybersecurity risks and incidents and developing State-wide cyber threat information analysis and dissemination activities;

[(4)**]** *(5)* purchasing, upgrading, storing, or maintaining equipment, including computer hardware and software;

[(5)**]** *(6)* ensuring operability and achieving interoperability of emergency communications;

[(6)] *(7)* responding to an increase in the threat level under the Homeland Security Advisory System, or to the needs resulting from a National Special Security Event;

[(7)] *(8)* establishing, enhancing, and staffing with appropriately qualified personnel State, local, and regional fusion centers that comply with the guidelines established under section 210A(i);

[(8)] *(9)* enhancing school preparedness;

[(9)] *(10)* enhancing the security and preparedness of secure and nonsecure areas of eligible airports and surface transportation systems;

[(10)] *(11)* supporting public safety answering points;

[(11)] *(12)* paying salaries and benefits for personnel, including individuals employed by the grant recipient on the date of the relevant grant application, to serve as qualified intelligence analysts, regardless of whether such analysts are current or new full-time employees or contract employees;

[(12)] *(13)* paying expenses directly related to administration of the grant, except that such expenses may not exceed 3 percent of the amount of the grant;

[(13)] *(14)* any activity permitted under the Fiscal Year 2007 Program Guidance of the Department for the State Homeland Security Grant Program, the Urban Area Security Initiative (including activities permitted under the full-time counterterrorism staffing pilot), or the Law Enforcement Terrorism Prevention Program; and

[(14)] *(15)* any other appropriate activity, as determined by the Administrator.

(b) LIMITATIONS ON USE OF FUNDS.—

(1) IN GENERAL.—Funds provided under section 2003 or 2004 may not be used—

(A) to supplant State or local funds, except that nothing in this paragraph shall prohibit the use of grant funds provided to a State or high-risk urban area for otherwise permissible uses under subsection (a) on the basis that a State or high-risk urban area has previously used State or local funds to support the same or similar uses; or

(B) for any State or local government cost-sharing contribution.

(2) PERSONNEL.—

(A) IN GENERAL.—Not more than 50 percent of the amount awarded to a grant recipient under section 2003 or 2004 in any fiscal year may be used to pay for personnel, including overtime and backfill costs, in support of the permitted uses under subsection (a).

(B) WAIVER.—At the request of the recipient of a grant under section 2003 or 2004, the Administrator may grant a waiver of the limitation under subparagraph (A).

(3) LIMITATIONS ON DISCRETION.—

(A) IN GENERAL.—With respect to the use of amounts awarded to a grant recipient under section 2003 or 2004 for personnel costs in accordance with paragraph (2) of this subsection, the Administrator may not—

(i) impose a limit on the amount of the award that may be used to pay for personnel, or personnel-re-

lated, costs that is higher or lower than the percent limit imposed in paragraph (2)(A); or

(ii) impose any additional limitation on the portion of the funds of a recipient that may be used for a specific type, purpose, or category of personnel, or personnel-related, costs.

(B) ANALYSTS.—If amounts awarded to a grant recipient under section 2003 or 2004 are used for paying salary or benefits of a qualified intelligence analyst under subsection (a)(10), the Administrator shall make such amounts available without time limitations placed on the period of time that the analyst can serve under the grant.

(4) CONSTRUCTION.—

(A) IN GENERAL.—A grant awarded under section 2003 or 2004 may not be used to acquire land or to construct buildings or other physical facilities.

(B) EXCEPTIONS.—

(i) IN GENERAL.—Notwithstanding subparagraph (A), nothing in this paragraph shall prohibit the use of a grant awarded under section 2003 or 2004 to achieve target capabilities related to preventing, preparing for, protecting against, or responding to acts of terrorism, including through the alteration or remodeling of existing buildings for the purpose of making such buildings secure against acts of terrorism.

(ii) REQUIREMENTS FOR EXCEPTION.—No grant awarded under section 2003 or 2004 may be used for a purpose described in clause (i) unless—

(I) specifically approved by the Administrator;

(II) any construction work occurs under terms and conditions consistent with the requirements under section 611(j)(9) of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5196(j)(9)); and

(III) the amount allocated for purposes under clause (i) does not exceed the greater of $1,000,000 or 15 percent of the grant award.

(5) RECREATION.—Grants awarded under this subtitle may not be used for recreational or social purposes.

(c) MULTIPLE-PURPOSE FUNDS.—Nothing in this subtitle shall be construed to prohibit State, local, or tribal governments from using grant funds under sections 2003 and 2004 in a manner that enhances preparedness for disasters unrelated to acts of terrorism, if such use assists such governments in achieving target capabilities related to preventing, preparing for, protecting against, or responding to acts of terrorism.

(d) REIMBURSEMENT OF COSTS.—

(1) PAID-ON-CALL OR VOLUNTEER REIMBURSEMENT.—In addition to the activities described in subsection (a), a grant under section 2003 or 2004 may be used to provide a reasonable stipend to paid-on-call or volunteer emergency response providers who are not otherwise compensated for travel to or participation in training or exercises related to the purposes of this subtitle. Any such reimbursement shall not be considered compensation for purposes of rendering an emergency response

provider an employee under the Fair Labor Standards Act of 1938 (29 U.S.C. 201 et seq.).

(2) PERFORMANCE OF FEDERAL DUTY.—An applicant for a grant under section 2003 or 2004 may petition the Administrator to use the funds from its grants under those sections for the reimbursement of the cost of any activity relating to preventing, preparing for, protecting against, or responding to acts of terrorism that is a Federal duty and usually performed by a Federal agency, and that is being performed by a State or local government under agreement with a Federal agency.

(e) FLEXIBILITY IN UNSPENT HOMELAND SECURITY GRANT FUNDS.—Upon request by the recipient of a grant under section 2003 or 2004, the Administrator may authorize the grant recipient to transfer all or part of the grant funds from uses specified in the grant agreement to other uses authorized under this section, if the Administrator determines that such transfer is in the interests of homeland security.

(f) EQUIPMENT STANDARDS.—If an applicant for a grant under section 2003 or 2004 proposes to upgrade or purchase, with assistance provided under that grant, new equipment or systems that do not meet or exceed any applicable national voluntary consensus standards developed under section 647 of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 747), the applicant shall include in its application an explanation of why such equipment or systems will serve the needs of the applicant better than equipment or systems that meet or exceed such standards.

* * * * * * *

○