114TH CONGRESS
1st Session
HOUSE OF REPRESENTATIVES
REPORT
114–284

DEPARTMENT OF HOMELAND SECURITY CYBERSECURITY STRATEGY ACT OF 2015

OCTOBER 6, 2015.—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. 3510]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security, to whom was referred the bill (H.R. 3510) to amend the Homeland Security Act of 2002 to require the Secretary of Homeland Security to develop a cybersecurity strategy for the Department of Homeland Security, and for other purposes, having considered the same, reports favorably thereon with an amendment and recommends that the bill as amended do pass.

CONTENTS

59–006

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 "Department of Homeland Security Cybersecurity Strategy Act of 2015".

SEC. 2. CYBERSECURITY STRATEGY FOR THE DEPARTMENT OF HOMELAND SECURITY.

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002 (6 U.S.C. 141 et seq.) is amended by adding at the end the following new section:

"SEC. 230. CYBERSECURITY STRATEGY.

"(a) IN GENERAL.—Not later than 60 days after the date of the enactment of this section, the Secretary shall develop a departmental strategy to carry out cybersecurity responsibilities as set forth in law.

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

"(1) Strategic and operational goals and priorities to successfully execute the full range of the Secretary's cybersecurity responsibilities.

"(2) Information on the programs, policies, and activities that are required to successfully execute the full range of the Secretary's cybersecurity responsibilities, including programs, policies, and activities in furtherance of the following:

"(A) Cybersecurity functions set forth in the second section 226 (relating to the national cybersecurity and communications integration center).

"(B) Cybersecurity investigations capabilities.

"(C) Cybersecurity research and development.

"(D) Engagement with international cybersecurity partners.

"(c) CONSIDERATIONS.—In developing the strategy required under subsection (a), the Secretary shall—

"(1) consider—

"(A) the cybersecurity strategy for the Homeland Security Enterprise published by the Secretary in November 2011;

"(B) the Department of Homeland Security Fiscal Years 2014 2018 Strategic Plan; and

"(C) the most recent Quadrennial Homeland Security Review issued pursuant to section 707; and

"(2) include information on the roles and responsibilities of components and offices of the Department, to the extent practicable, to carry out such strategy.

"(d) IMPLEMENTATION PLAN.—Not later than 90 days after the development of the strategy required under subsection (a), the Secretary shall issue an implementation plan for the strategy that includes the following:

"(1) Strategic objectives and corresponding tasks.

"(2) Projected timelines and costs for such tasks.

"(3) Metrics to evaluate performance of such tasks.

"(e) CONGRESSIONAL OVERSIGHT.—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 for assessment the following:

"(1) A copy of the strategy required under subsection (a) upon issuance.

"(2) A copy of the implementation plan required under subsection (d) upon issuance, together with detailed information on any associated legislative or budgetary proposals.

"(f) PROHIBITION ON REORGANIZATION.—In the event that the strategy required under subsection (a) or implementation plan required under subsection (d) includes actions to reorganize departmental components or offices, such actions may not be executed without prior congressional authorization.

"(g) CLASSIFIED INFORMATION.—The strategy required under subsection (a) shall be in an unclassified form but may contain a classified annex.

"(h) RULE OF CONSTRUCTION.—Nothing in this section may be construed as permitting the Department to engage in monitoring, surveillance, exfiltration, or other collection activities for the purpose of tracking an individual's personally identifiable information.

"(i) DEFINITIONS.—In this section:

"(1) CYBERSECURITY RISK.—The term 'cybersecurity risk' has the meaning given such term in the second section 226, relating to the national cybersecurity and communications integration center.

"(2) HOMELAND SECURITY ENTERPRISE.—The term 'Homeland Security Enterprise' means relevant governmental and nongovernmental entities involved in homeland security, including Federal, State, local, and tribal government officials, private sector representatives, academics, and other policy experts.

"(3) INCIDENT.—The term 'incident' has the meaning given such term in the second section 226, relating to the national cybersecurity and communications integration center.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by adding at the end of the list of items for subtitle C of title II the following new item:

"Sec. 230. Cybersecurity strategy.".

(c) AMENDMENT TO DEFINITION.—Paragraph (2) of subsection (a) of the second section 226 of the Homeland Security Act of 2002 (6 U.S.C. 148; relating to the national cybersecurity and communications integration center) is amended to read as follows:

"(2) 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;".

PURPOSE AND SUMMARY

The purpose of H.R. 3510 is to amend the Homeland Security Act of 2002 to instruct the Secretary of the Department of Homeland Security (Department or DHS) to develop a departmental cybersecurity strategy and implementation plan to carry out the cybersecurity responsibilities of the department and to prohibit the department from reorganizing or realigning offices within the National Protection and Programs Directorate without Congressional approval.

BACKGROUND AND NEED FOR LEGISLATION

Cyber attacks stand to disrupt the operations of government, businesses, and the lives of the American people. Increasingly sophisticated cyber threats have underscored the need to manage and strengthen the cybersecurity of the nation's critical infrastructure. The Government Accountability Office (GAO) recommended that an overarching Federal cybersecurity strategy be implemented and that such strategy should define key elements of a national strategy including roles and responsibilities. H.R. 3510 ensures DHS develops such a strategy.

On September 4, 2015, the Department's Inspector General issued a report entitled "DHS Can Strengthen Its Cyber Mission Coordination Efforts'" that recommended that DHS develop a comprehensive, cross-departmental strategic implementation plan that defines components' cyber missions and responsibilities, including long-term goals, performance metrics, and milestones to measure progress in unifying the Department's incident response and coordination efforts" (DHS–OIG–15–140). H.R. 3510 directs the Department to develop a department-wide strategy and implementation plan to ensure performance of its multi-faceted cybersecurity mission.

At present, efforts are underway within the Department for a wide-scale reorganization of the National Protection and Programs Directorate (NPPD). It is critical that Congress be a legislative proposal to determine whether or not the proposed changes would provide a clear mission, streamline the organization's structure, and ensure a qualified workforce to successfully carry out its mission. H.R. 3510 also seeks to ensure such congressional oversight by requiring congressional authorization for any such action.

The Committee is concerned with the lack of transparency on the Department's efforts to reorganize to carry out its cybersecurity and infrastructure protection missions. The Committee communicated this concern to the Secretary of Homeland Security in a letter sent September 15, 2015, and made it clear that any reorganization or realignment will require Congressional authorization. Given this Committee's legislative and oversight efforts to strengthen Departmental cybersecurity functions, it's essential that DHS submit any proposal to Congress prior to reorganization or realignment. Congressional interest is evident in the numerous pieces of legislation this Committee has considered and hearings this Committee has conducted.

HEARINGS

The Committee on Homeland Security did not hold any legislative hearings on H.R. 3510, however the Committee held oversight hearings listed below.

On February 12, 2015, the Subcommittee held a hearing entitled "Emerging Threats and Technologies to Protect the Homeland." The Subcommittee received testimony from Mr. Andy Ozment, Assistant Secretary, Office of Cybersecurity and Communications, National Protection and Programs Directorate, U.S. Department of Homeland Security; Dr. Huban Gowadia, Director, Domestic Nuclear Detection Office, U.S. Department of Homeland Security; Mr. Joseph Martin, Acting Director, Homeland Security Enterprise and First Responders Group, Science and Technology Directorate, U.S. Department of Homeland Security; Mr. William Noonan, Deputy Special Agent in Charge, Criminal Investigative Division, Cyber Operations Branch, United States Secret Service, U.S. Department of Homeland Security; and Mr. William Painter, Analyst, Government and Finance Division, Congressional Research Service, Library of Congress.

On March 4, 2015, the Subcommittee held a hearing entitled "Industry Perspectives on the President's Cybersecurity Information Sharing Proposal." The Subcommittee received testimony from Mr. Matthew J. Eggers, Senior Director, National Security and Emergency Preparedness, U.S. Chamber of Commerce; Ms. Mary Ellen Callahan, Jenner & Block and the Former Chief Privacy Officer, U.S. Department of Homeland Security; Mr. Gregory T. Garcia, Executive Director, Financial Services Sector Coordinating Council; and Dr. Martin Libicki, The RAND Corporation.

On June 24, 2015, the Subcommittee held a hearing entitled "DHS' Efforts to Secure .Gov." The Subcommittee received testimony from Dr. Andy Ozment, Assistant Secretary, Office of Cybersecurity and Communications, National Protections and Programs Directorate, U.S. Department of Homeland Security; Mr. Gregory C. Wilshusen, Director, Information Security Issues, Government Accountability Office; and Dr. Daniel M. Gerstein, The RAND Corporation.

COMMITTEE CONSIDERATION

The Committee met on September 30, 2015, to consider H.R. 3510, 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 offered by MR. CLAWSON (#1); was AGREED TO by voice vote.

Page 5, line 4, insert a new clause entitled "(h) Rule of Construction."

The Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies met on September 17, 2015, to consider H.R. 3510 and reported the measure 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. 3510.

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. 3510, the Department of Homeland Security Cybersecurity Strategy Act of 2015, 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, October 5, 2015.

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. 3510, the Department of Homeland Security Cybersecurity Strategy Act of 2015.

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

Sincerely,

KEITH HALL.

Enclosure.

H.R. 3510—Department of Homeland Security Cybersecurity Strategy Act of 2015

H.R. 3510 would require the Department of Homeland Security (DHS), within 60 days of the bill's enactment, to develop a strategy to execute the department's cybersecurity responsibilities under current law. The bill also would require DHS to issue a plan to implement that strategy not later than 90 days after the strategy is developed and to deliver the strategy and the plan to the Congress. Because DHS is currently developing a cybersecurity strategy and would be able to meet the deadlines established in the bill, CBO estimates that implementing the bill would not have a significant effect on the budget.

Enacting H.R. 3510 would not affect direct spending or revenues; therefore, pay-as-you-go procedures do not apply.

H.R. 3510 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act and would not affect the budgets of state, local, or tribal governments.

The CBO staff contact for this estimate is William Ma. 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. 3510 contains the following general performance goals and objectives, including outcome related goals and objectives authorized.

This legislation requires the Secretary of Homeland Security to develop a cybersecurity strategy for the Department of Homeland Security (DHS) and to submit such strategy to Congress no later than 60 days after the enactment of this legislation. The Secretary is also directed to submit an implementation plan for the cybersecurity strategy 90 days after the development of the strategy. Additionally, this legislation would clarify the requirement for DHS to submit proposals to Congress prior to reorganization or realignment. H.R. 3510 helps to strengthen the security and resiliency of cyberspace by requiring the Secretary to thoroughly examine the goals, priorities, roles, and responsibilities that are necessary to execute its mission. The development of a strategy will ensure the Secretary considers cybersecurity functions across the Department holistically in order to more effectively achieve the cybersecurity priorities of the Department.

Efforts are presently underway within the Department for a wide-scale reorganization of the National Protection and Programs Directorate (NPPD). It is critical that Congress be provided a legislative proposal to determine whether or not the proposed changes would provide a clear mission, streamline the organization's structure, and ensure a qualified workforce to successfully carry out its mission. H.R. 3510 also seeks to ensure proper oversight and transparency and reflects the appropriate roles of both the Legislative and Executive branches of the Government.

DUPLICATIVE FEDERAL PROGRAMS

Pursuant to clause 3(c) of rule XIII, the Committee finds that H.R. 3510 does not contain any provision that establishes or reau-

thorizes 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. 3510 does not preempt any State, local, or Tribal law.

DISCLOSURE OF DIRECTED RULE MAKINGS

The Committee estimates that H.R. 3510 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 bill may be cited as the "Department of Homeland Security Cybersecurity Strategy Act of 2015".

Section 2. Cybersecurity strategy for the Department of Homeland Security

(a) Subtitle C of title II of the Homeland Security Act of 2002 is amended to add the following new section:

"SEC. 230. CYBERSECURITY STRATEGY."

(a) IN GENERAL.

This subsection directs the Secretary of the Department of Homeland Security to develop a departmental strategy to carry out cybersecurity responsibilities as set forth in law.

(b) CONTENTS OF STRATEGY.

This subsection details the contents of the strategy to include the strategic and operational goals and priorities needed to execute the Department's cybersecurity responsibilities including information on its programs, policies, and activities. These programs, policies, and activities should include the Department's cybersecurity functions set forth in the second section 226 of the Homeland Security Act (HSA), cybersecurity investigations capabilities, cybersecurity research and development, and engagement with international cybersecurity partners.

Cybersecurity functions set forth in the second section 226 of the HSA include: (1) Being a Federal civilian interface for the multidirectional and cross-sector sharing of information related to cybersecurity risks, incidents, analysis, and warnings for Federal and non-Federal entities; (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 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 cybersecurity risks and incidents; and (B) sharing the analysis conducted under subparagraph (A) with Federal and non Federal entities; (6) upon request, providing timely technical assistance, risk management support, and incident response capabilities to Federal and non-Federal entities with respect to cybersecurity risks and incidents, which may include attribution, mitigation, and remediation; and (7) providing information and recommendations on security and resilience measures to Federal and non-Federal entities, including information and recommendations to: (A) facilitate information security; and (B) strengthen information systems against cybersecurity risks and incidents.

(c) CONSIDERATIONS.

This subsection requires the Secretary to consider other DHS strategic documents when developing the cybersecurity strategy including the cybersecurity strategy for the Homeland Security Enterprise published by the Secretary in November 2011, the Department of Homeland Security Fiscal Years 2014–2018 Strategic Plan, the most recent Quadrennial Homeland Security Review issued pursuant to section 707 of the HAS. It must also include information on the roles and responsibilities of components and offices across the Department when developing the strategy.

(d) IMPLEMENTATION PLAN.

The Secretary is required no later than 90 days to develop a plan for implementing the strategy that includes strategic objectives and

corresponding tasks, projected timelines and costs for such tasks, and metrics to evaluate performance.

(e) CONGRESSIONAL OVERSIGHT.

This subsection requires the Secretary to submit the required strategy and the implementation plan, along with information on any associated legislative or budgetary proposals, to the House Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate for an assessment.

(f) PROHIBITION OF REORGANIZATION.

The Committee intends this subsection to prohibit the reorganization or realignment of NPPD without Congressional authorization. It is the role of the legislative branch to authorize and appropriate dollars for the Department of Homeland Security. In particular, it is this Committee's role and responsibility to legislate and oversee Department activities.

The Committee has previously reviewed Administrative legislative proposals and worked with DHS to authorize various cyber programs. For example; S. 2521, the Federal Information Security Modernization Act of 2014, in which the Secretary of Homeland Security was given authority to administer the implementation of information security policies and practices, H.R. 2952, the Cybersecurity Workforce Assessment Act, in which the Secretary was directed to conduct an assessment of the cybersecurity workforce of the Department of Homeland Security, H.R. 3696 which established the National Cybersecurity and Communications Integration Center (NCCIC) and required that the Secretary of Homeland Security conduct cybersecurity activities, H.R. 3107 which directed the Secretary to develop a workforce strategy that enhances the readiness, capacity, training, recruitment, and retention of the DHS cybersecurity workforce, and H.R. 1731 which would rename NPPD as Cybersecurity and Infrastructure Protection and codify a Deputy Under Secretary for Cybersecurity and a Deputy Under Secretary for Infrastructure Protection. These and other efforts serve to represent the important role of Congressional oversight.

(g) CLASSIFIED INFORMATION.

This subsection requires that the proposed plan must be available in an unclassified form, but that it may have a classified annex.

(h) RULE OF CONSTRUCTION.

This subsection ensures that nothing in this act can be construed to permit the Department to engage in monitoring, surveillance, exfiltration, or other collection activities for the purpose of tracking an individual's personally identifiable information.

(i) DEFINITIONS.

This subsection defines "cybersecurity risk" and "incident" as the meaning given to both in the second section 226 relating to the national cybersecurity and communications integration. "Homeland Security Enterprise" is defined as the relevant governmental and nongovernmental entities involved in homeland security, including Federal, State, local, and tribal governmental officials, private sector representatives, academics, and other policy experts.

(b) Clerical Amendment.

This subsection amends the table of contents of the Homeland Security Act of 2002.

(c) Amendment to Definition.

This subsection strikes and replaces the definition of "incident" in the second section 226 of the Homeland Security Act to mean an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentially, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

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

HOMELAND SECURITY ACT OF 2002

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

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

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

* * * * * * *

TITLE V—NATIONAL EMERGENCY MANAGEMENT

* * * * * * *

Sec. 230. Cybersecurity strategy.

* * * * * * *

TITLE II—INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION

* * * * * * *

Subtitle C—Information Security

* * * * * * *

SEC. 226. NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER.

(a) DEFINITIONS.—In this section—

(1) the term "cybersecurity risk" 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 information or information systems, including such related consequences caused by an act of terrorism;

[(2) the term "incident" means an occurrence that—

[(A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system; or

[(B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies;]

(2) 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;

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

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

(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 cybersecurity risks, incidents, analysis, and warnings for Federal and non-Federal entities;

(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 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 cybersecurity risks and incidents; and

(B) sharing the analysis conducted under subparagraph (A) with Federal and non-Federal entities;

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

(7) providing information and recommendations on security and resilience measures to Federal and non-Federal entities, including information and recommendations to—

(A) facilitate information security; and

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

(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 and local governments;

(ii) information sharing and analysis organizations; and

(iii) owners and operators of critical information systems;

(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; and

(E) 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 information related to cybersecurity risks, incidents, and analysis is shared;

(B) when appropriate, 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 cybersecurity risks and incidents that are technology-neutral, interoperable, real-time, cost-effective, and resilient; and

(G) the Center works with other agencies to reduce unnecessarily duplicative sharing of information related to cybersecurity risks and incidents;

(2) that information related to cybersecurity risks and incidents is appropriately safeguarded against unauthorized access; 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.

(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.

* * * * * * *

SEC. 230. CYBERSECURITY STRATEGY.

(a) IN GENERAL.—Not later than 60 days after the date of the enactment of this section, the Secretary shall develop a departmental strategy to carry out cybersecurity responsibilities as set forth in law.

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

(1) Strategic and operational goals and priorities to successfully execute the full range of the Secretary's cybersecurity responsibilities.

(2) Information on the programs, policies, and activities that are required to successfully execute the full range of the Secretary's cybersecurity responsibilities, including programs, policies, and activities in furtherance of the following:

(A) Cybersecurity functions set forth in the second section 226 (relating to the national cybersecurity and communications integration center).

(B) Cybersecurity investigations capabilities.

(C) Cybersecurity research and development.

(D) Engagement with international cybersecurity partners.

(c) CONSIDERATIONS.—In developing the strategy required under subsection (a), the Secretary shall—

(1) consider—

(A) the cybersecurity strategy for the Homeland Security Enterprise published by the Secretary in November 2011;

(B) the Department of Homeland Security Fiscal Years 2014 2018 Strategic Plan; and

(C) the most recent Quadrennial Homeland Security Review issued pursuant to section 707; and

(2) include information on the roles and responsibilities of components and offices of the Department, to the extent practicable, to carry out such strategy.

(d) IMPLEMENTATION PLAN.—Not later than 90 days after the development of the strategy required under subsection (a), the Sec-

retary shall issue an implementation plan for the strategy that includes the following:

(1) Strategic objectives and corresponding tasks.

(2) Projected timelines and costs for such tasks.

(3) Metrics to evaluate performance of such tasks.

(e) CONGRESSIONAL OVERSIGHT.—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 for assessment the following:

(1) A copy of the strategy required under subsection (a) upon issuance.

(2) A copy of the implementation plan required under subsection (d) upon issuance, together with detailed information on any associated legislative or budgetary proposals.

(f) PROHIBITION ON REORGANIZATION.—In the event that the strategy required under subsection (a) or implementation plan required under subsection (d) includes actions to reorganize departmental components or offices, such actions may not be executed without prior congressional authorization.

(g) CLASSIFIED INFORMATION.—The strategy required under subsection (a) shall be in an unclassified form but may contain a classified annex.

(h) RULE OF CONSTRUCTION.—Nothing in this section may be construed as permitting the Department to engage in monitoring, surveillance, exfiltration, or other collection activities for the purpose of tracking an individual's personally identifiable information.

(i) DEFINITIONS.—In this section:

(1) CYBERSECURITY RISK.—

The term "cybersecurity risk" has the meaning given such term in the second section 226, relating to the national cybersecurity and communications integration center.

(2) HOMELAND SECURITY ENTERPRISE.—

The term "Homeland Security Enterprise" means relevant governmental and nongovernmental entities involved in homeland security, including Federal, State, local, and tribal government officials, private sector representatives, academics, and other policy experts.

(3) INCIDENT.—

The term "incident" has the meaning given such term in the second section 226, relating to the national cybersecurity and communications integration center.

○