114TH CONGRESS
1ST SESSION

H. R. 3510

IN THE SENATE OF THE UNITED STATES

OCTOBER 7, 2015

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

AN ACT

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.

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

SECTION 1. SHORT TITLE.

This Act may be cited as the ''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) CLASSIFIED INFORMATION.—The strategy required under subsection (a) shall be in an unclassified form but may contain a classified annex.

''(g) 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.

''(h) 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) PROHIBITION ON REORGANIZATION.—The Secretary of Homeland Security may not change the location or reporting structure of the National Protection and Programs Directorate of the Department of Homeland Security, or the location or reporting structure of any office

or component of the Directorate, unless the Secretary receives prior authorization from Congress permitting such change.

(c) 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.".

(d) 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;".

Passed the House of Representatives October 6, 2015.

Attest: KAREN L. HAAS,

Clerk.