I

113TH CONGRESS
1ST SESSION

H. R. 2556

To provide for the establishment of Vertical Centers of Excellence on Cybersecurity to create solutions to, and promote best practices for, industry-specific cybersecurity challenges.

IN THE HOUSE OF REPRESENTATIVES

JUNE 27, 2013

Mr. HONDA introduced the following bill; which was referred to the Committee on Science, Space, and Technology

---

A BILL

To provide for the establishment of Vertical Centers of Excellence on Cybersecurity to create solutions to, and promote best practices for, industry-specific cybersecurity challenges.

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 ‘‘Excellence in Cybersecurity Act’’.

SEC. 2. FINDINGS.

Congress finds the following:

(1) Cybercrime is one of the preeminent threats facing the United States today, and presents a cumulative national security, economic, and individual threat unlike any before it.

(2) The total global cost of cybercrime is estimated to be $1,000,000,000,000 per year and represents one of the greatest transfers of wealth in the history of the world.

(3) Cybercrime surveys have found that the solutions to cybersecurity threats are multi-pronged and go beyond increased data sharing and threat analysis.

(4) Many leaders of organizations do not know who is responsible for the cybersecurity needs of their organization or industry. These leaders also underestimate the capabilities of their adversaries in cybercrime and the strategic, financial, reputational, and regulatory risks those adversaries pose to organizations.

(5) Security experts are not effectively communicating best practices to address cyberthreats, cyberattacks, and defensive technologies.

(6) Cybersecurity experts believe there are 4 key factors that impact the vulnerability of an organization to cybercrime:

(A) Understanding the changes to and best practices for the current threat environment.

(B) Strategy and execution of a cybersecurity program.

(C) The identification of key assets in need of protection.

(D) The ability to develop relationships with similar organizations to develop protection within the industry ecosystem.

(7) It is essential that the United States prioritize the development of organizational relationships and best practices of specific industries to help protect those industries against threats to cybersecurity.

SEC. 3. VERTICAL CENTERS OF EXCELLENCE ON CYBERSECURITY.

(a) ESTABLISHMENT.—The Director of the National Institute of Standards and Technology shall establish 5 Vertical Centers of Excellence on Cybersecurity.

(b) MISSION.—Each Center shall convene experts and individuals in the industry that is the focus of the work of that Center for the purposes of—

(1) identifying and analyzing existing and future cybersecurity challenges faced by various industries;

(2) creating solutions and promoting best practices to address such challenges; and

(3) collaborating with individuals in those industries to share knowledge.

(c) REQUIREMENTS.—In establishing each Center under subsection (a), the Director, not later than 6 months after the date of enactment of this Act, shall select—

(1) a particular industry that faces cybersecurity challenges to be the focus of the work of that Center;

(2) a manager to be responsible for the administrative functions of that Center; and

(3) the location of that Center pursuant to subsection (d).

(d) LOCATION REQUIREMENTS.—The Director shall seek to ensure that each Center is located a sufficient geographical distance from another Center and shall select a location for each Center based on—

(1) proximity to the geographical location of a number of businesses operating in the industry selected pursuant to subsection (c)(1);

(2) accessibility to the experts selected pursuant to section 5; and

(3) the capacity of the facilities at the Center to convene, and promote collaboration among, experts and individuals in that industry.

(e) PARTNERSHIPS.—The Director may establish partnerships with public or nonprofit entities to provide services for a Center established under subsection (a).

SEC. 4. DUTIES OF CENTERS.

(a) IN GENERAL.—The Director and the manager of each Center shall jointly select a group of experts, consistent with the requirements in section 5, to carry out the duties described in subsection (b).

(b) DUTIES OF EXPERTS.—The experts at each Center shall—

(1) identify and analyze existing and future cybersecurity challenges faced by the industry selected pursuant to section 2(c)(1);

(2) create solutions to those cybersecurity challenges that are cost-effective, repeatable, and scalable;

(3) collaborate, convene discussions, and share knowledge with individuals in that industry to accomplish the work of the Center; and

(4) create educational programs to promote best practices in cybersecurity for such individuals.

(c) REQUIREMENTS OF CENTERS.—Each Center shall—

(1) work within the Cybersecurity Framework created pursuant to section 7 of Executive Order 13636, entitled ‘‘Improving Critical Infrastructure Cybersecurity’’ (78 Fed. Reg. 11739);

(2) collaborate with each of the other Centers to share relevant information;

(3) encourage the development of relationships among individuals in the industry selected pursuant to section 2(c)(1); and

(4) share the best practices and lessons learned from the work of the Center with those individuals.

(d) CONFIDENTIALITY.—The Director, in consultation with individuals in the industry selected pursuant to section 2(c)(1), shall establish procedures to ensure the confidentiality of the information handled by the Centers. The Centers shall be exempt from the requirements set forth in section 552(b) of title 5, United States Code (commonly known as the Freedom of Information Act).

SEC. 5. REQUIREMENTS FOR EXPERTS.

(a) NUMBER AND COMPENSATION.—The Director shall determine—

(1) the number of experts at each Center; and

(2) the compensation for each expert selected.

(b) QUALIFICATIONS.—Experts shall have experience in government, academia, or the particular industry that is the focus of the work of the Center, and any other qualifications the Director may determine.

SEC. 6. REPORT.

Not later than 1 year after the date of enactment of this Act, the Director shall submit a report to Congress describing the cybersecurity challenges, solutions, and best practices addressed by each Center.

SEC. 7. DEFINITIONS.

In this Act:

(1) CENTER.—The term ''Center'' means a Vertical Center of Excellence on Cybersecurity established under section 2(a).

(2) DIRECTOR.—The term ''Director'' means the Director of the National Institute of Standards and Technology.

SEC. 8. AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated to the Director for each of fiscal years 2014 through 2019 $25,000,000 to carry out this Act. Amounts appropriated pursuant to this section shall be subdivided into 5 equal amounts to be distributed to each Center.

○