

CYBERSECURITY EDUCATION ENHANCEMENT ACT OF
2008

SEPTEMBER 8, 2008.—Ordered to be printed

Mr. THOMPSON of Mississippi, from the Committee on Homeland
Security, submitted the following

R E P O R T

[To accompany H.R. 263]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security, to whom was referred the bill (H.R. 263) to authorize the Secretary of Homeland Security to establish a program to award grants to institutions of higher education for the establishment or expansion of cybersecurity professional development programs, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

Purpose and Summary	Page 00
Background and Need for Legislation	00
Hearings	00
Committee Consideration	00
Committee Votes	00
Committee Oversight Findings	00
New Budget Authority, Entitlement Authority, and Tax Expenditures	00
Congressional Budget Office Estimate	00
Statement of General Performance Goals and Objectives	00
Congressional Earmarks, Limited Tax Benefits, and Limited Tariff Benefits ...	00
Federal Mandates Statement	00
Advisory Committee Statement	00
Constitutional Authority Statement	00
Applicability to Legislative Branch	00
Section-by-Section Analysis of the Legislation	00
Changes in Existing Law Made by the Bill, as Reported	00

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 “Cybersecurity Education Enhancement Act of 2008”.

SEC. 2. DEPARTMENT OF HOMELAND SECURITY CYBERSECURITY TRAINING PROGRAMS AND EQUIPMENT.

(a) **IN GENERAL.**—The Secretary of Homeland Security, acting through the Assistant Secretary of Cybersecurity and subject to the availability of appropriations, shall establish a program to award grants to institutions of higher education (and consortia thereof) for—

- (1) the establishment or expansion of cybersecurity professional development programs;
- (2) the establishment or expansion (or both) of associate degree programs in cybersecurity; and
- (3) the purchase of equipment to provide training in cybersecurity for professional development programs and degree programs.

(b) **GOALS AND CRITERIA.**—The Secretary, acting through the Assistant Secretary—

- (1) shall establish the goals and criteria for the program established under this section and the criteria for awarding grants under such program; and
- (2) shall operate the program consistent with the goals and criteria established under paragraph (1), including soliciting applicants, reviewing applications, and making and administering awards.

(c) **GRANT AWARDS.**—

(1) **PEER REVIEW.**—All grant awards under this section shall be provided on a competitive, merit-reviewed basis.

(2) **FOCUS.**—In awarding grants under this section, the Secretary shall, to the extent practicable, ensure geographic diversity and the participation of women and underrepresented minorities.

(3) **PREFERENCE.**—In awarding grants under this section, the Secretary—

(A) shall give preference to applications submitted by consortia of institutions, to encourage as many students and professionals as possible to benefit from the program established under this section; and

(B) shall give preference to any application submitted by a consortium of institutions that includes at least one institution of higher education that is eligible to receive funds under title III or V of the Higher Education Act of 1965.

(d) **INSTITUTION OF HIGHER EDUCATION DEFINED.**—In this section the term “institution of higher education” has the meaning given that term in section 101(a) of the Higher Education Act of 1965 (20 U.S.C. 1001(a)).

(e) **AUTHORIZATION OF APPROPRIATIONS.**—There is authorized to be appropriated to the Secretary for carrying out this section \$5,000,000 for each of fiscal years 2009 and 2010.

SEC. 3. DHS CYBERSECURITY FELLOWS PROGRAM.

(a) **ESTABLISHMENT OF PROGRAM.**—Subtitle C of title II of the Homeland Security Act of 2002 (6 U.S.C. 121 et seq.) is amended by adding at the end the following:

“SEC. 226. DHS CYBERSECURITY FELLOWS PROGRAM.

“(a) **ESTABLISHMENT.**—

“(1) **IN GENERAL.**—The Secretary shall establish a fellowship program in accordance with this section for the purpose of bringing State, local, tribal, and private sector officials to participate in the work of the National Cybersecurity Division in order to assist with the Department’s stated cybersecurity missions and capabilities, including—

“(A) enhancing Federal, State, local, and tribal government cybersecurity;

“(B) developing partnerships with other Federal agencies, State, local, and tribal governments, and the private sector;

“(C) improving and enhancing public/private information sharing involving information regarding cyber attacks, threats, and vulnerabilities;

“(D) providing and coordinating incident response and recovery planning efforts; and

“(E) fostering training and certification.

“(2) **PROGRAM NAME.**—The program under this section shall be known as the DHS Cybersecurity Fellows Program.

“(b) **ELIGIBILITY.**—In order to be eligible for selection as a fellow under the program, an individual must—

“(1) have cybersecurity-related responsibilities;

“(2) be eligible to possess an appropriate national security clearance; and

- “(3) if the individual has, or is employed by a person that has, a contract with the Department or business before the Department, report to the Secretary any conflicts of interest of the individual with respect to such contract or business.
- “(c) LIMITATIONS.—The Secretary—
- “(1) may conduct up to 2 iterations of the program each year, each of which shall be 180 days in duration; and
- “(2) shall ensure that the number of fellows selected for each iteration does not impede the activities of the National Cybersecurity Division.
- “(d) CONDITION.—As a condition of selecting an individual as a fellow under the program, the Secretary shall verify that the individual’s employer agrees to continue to pay the individual’s salary and benefits during the period of the fellowship.
- “(e) STIPEND.—During the period of the fellowship of an individual under the program, the Secretary may, subject to the availability of appropriations, provide to the individual a stipend to cover the individual’s reasonable living expenses during the period of the fellowship.”.
- (b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by adding at the end of the items relating to such subtitle the following:
- “Sec. 226. DHS cybersecurity fellows program.”.

SEC. 4. SENSE OF CONGRESS—CYBERSECURITY.

It is the sense of the Congress that the House of Representatives should designate a committee to serve as the single, principal point of oversight and review for cybersecurity.

PURPOSE AND SUMMARY

The purpose of H.R. 263 is to authorize the Secretary of Homeland Security to establish a program to award grants to institutions of higher education for the establishment or expansion of cybersecurity professional development programs, and for other purposes.

BACKGROUND AND NEED FOR LEGISLATION

During the course of the 110th Congress, the Subcommittee on Emerging Threats, Cybersecurity, Science and Technology conducted dozens of hearings and investigations into cybersecurity issues affecting Federal and critical infrastructure networks, with the goal of increasing public awareness, fixing vulnerabilities, and holding individuals, agencies, and private sector entities responsible and accountable for their actions. One of the key vulnerabilities that the Committee has discovered is the lack of information security training and awareness across all levels and branches of American government and the private sector. This bill establishes a grant program to enable higher education institutions to develop or expand cybersecurity education programs. In addition, the bill provides opportunities for State, local, tribal, and private sector officials with cybersecurity expertise to work at the National Cybersecurity Division.

HEARINGS

No Committee hearings were held on H.R. 263, however the Committee held an oversight hearing on cybersecurity.

On April 25, 2007, the Subcommittee on Emerging Threats, Cybersecurity and Science and Technology held a hearing entitled “Addressing the Nation’s Cybersecurity Challenges: Reducing Vulnerabilities Requires Strategic Investment and Immediate Action.” The Subcommittee received testimony from Dr. Daniel E. Geer, Jr., Principal, Geer Risk Services, LLC; Dr. James Andrew Lewis, Director and Senior Fellow, Technology and Public Policy Program, Center for Strategic and International Studies; Dr. Doug-

las Maughan, Program Manager, Cyber Security R&D, science and Technology Directorate, Department of Homeland Security; and Mr. O. Sami Saydjari, President, Professionals for Cyber Defense Chief Executive Officer, Cyber Defense Agency, LLC.

COMMITTEE CONSIDERATION

In the 109th Congress H.R. 3109, the “Cybersecurity Education Enhancement Act of 2005” was introduced in the House by Ms. Jackson-Lee of Texas and four original co-sponsors.

H.R. 263 was introduced in the House on January 5, 2007, by Ms. Jackson-Lee of Texas and referred to the Committee on Science and Technology, and in addition to the Committee on Education and Labor and the Committee on Homeland Security. Within the Committee on Homeland Security, H.R. 263 was referred to the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology.

On June 26, 2008, the Chairman discharged the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology from further consideration of H.R. 263. The Full Committee then proceeded to the consideration of H.R. 263 and ordered the measure reported to the House, amended, with a favorable recommendation.

The Committee adopted the measure, as amended, by unanimous consent.

The following amendments were offered:

An Amendment in the Nature of a Substitute offered by Ms. Jackson-Lee (#1), was AGREED TO by unanimous consent.

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 Committee consideration.

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. 263, the Cybersecurity Education Enhancement Act of 2007, 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, August 21, 2008.

Hon. BENNIE G. THOMPSON,
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. 263, the Cybersecurity Education Enhancement Act of 2008.

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

Sincerely,

PETER H. FONTAINE
(For Peter R. Orszag, Director).

Enclosure.

H.R. 263—Cybersecurity Education Enhancement Act of 2008

Summary: H.R. 263 would authorize the appropriation of \$5 million for each of fiscal years 2009 and 2010 for the Department of Homeland Security (DHS) to make grants to institutions of higher education to establish or expand cybersecurity programs. In addition, the bill would direct DHS to establish a fellowship program for nonfederal employees to work temporarily in the department's National Cybersecurity Division. CBO estimates that implementing the bill would cost about \$11 million over the 2009–2013 period, subject to appropriation of the necessary amounts. Enacting H.R. 263 would not affect direct spending or revenues.

H.R. 263 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would impose no costs on state, local or tribal governments.

Estimated cost to the Federal Government: The estimated budgetary impact of H.R. 263 is shown in the following table. The costs of this legislation fall within budget function 750 (administration of justice).

Basis of estimate: For this estimate, CBO assumes that the necessary amounts will be appropriated near the start of each fiscal year and that outlays will follow the historical rate of spending for similar activities.

	By fiscal year, in millions of dollars—					
	2009	2010	2011	2012	2013	2009–2013
CHANGES IN SPENDING SUBJECT TO APPROPRIATION						
Estimated Authorization Level	5	5	*	*	*	11
Estimated Outlays	2	3	4	1	*	11

Note: * = less than \$500,000.

In addition to the specified authorizations of \$5 million for each of 2009 and 2010 for grants to expand cybersecurity programs, H.R. 263 would permit DHS to provide a stipend to cover reasonable living expenses for participants in the fellowship program established by the bill. CBO expects that about 20 people would participate in the new program in Washington, D.C., each year with each individual spending no more than six months in the program. We estimate that annual costs for stipends (including housing and

commuting expenses) could be a few hundred thousand dollars each year and would total about \$1 million over the 2009–2013 period, subject to the availability of appropriated funds.

Intergovernmental and private-sector impact: H.R. 263 contains no intergovernmental or private-sector mandates as defined in UMRA. The bill would benefit state, local and tribal governments by establishing grants for institutions of higher education and by creating a fellows program to provide training on cybersecurity issues and to foster partnerships on cybersecurity issues.

Estimate prepared by: Federal Costs: Mark Grabowicz; Impact on State, Local, and Tribal Governments: Burke Doherty; Impact on the Private Sector: Paige Piper/Bach.

Estimate approved by: Peter H. Fontaine, 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. 263, contains the following general performance goals, and objectives, including outcome related goals and objectives authorized.

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(d), 9(e), or 9(f) 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.

ADVISORY COMMITTEE STATEMENT

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

CONSTITUTIONAL AUTHORITY STATEMENT

Pursuant to clause 3(d)(1) of rule XIII of the Rules of the House of Representatives, the Committee finds that the Constitutional authority for this legislation is provided in Article I, section 8, clause 1, which grants Congress the power to provide for the common Defense of the United States.

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 cites the measure as the “Cybersecurity Education Enhancement Act of 2008.”

Section 2. Department of Homeland Security Cybersecurity training programs and equipment

This section establishes a program to award grants to institutions of higher education (and consortia thereof) for: (1) the establishment or expansion of cybersecurity professional development programs; (2) the establishment or expansion (or both) of associate degree programs in cybersecurity; and (3) the purchase of equipment to provide training in cybersecurity for either professional development programs or degree programs.

Section 3. DHS Cybersecurity Fellows Program

This section establishes a fellowship program for the purpose of bringing State, local, tribal, and private sector officials to participate in the work of the National Cybersecurity Division in order to assist with the Department’s stated cybersecurity missions and capabilities. In order to be eligible for selection as a fellow under the program, an individual must: (1) have cybersecurity-related responsibilities; and (2) be eligible to possess an appropriate National security clearance.

Section 4. Sense of Congress

This section states that it is the sense of the Congress that the House of Representatives and the Senate should designate a committee in each body to serve as the single, principal point of oversight and review for cybersecurity. Because cybersecurity is an issue of great economic and National importance, the Committee believes that the House of Representatives must reorganize and realign the committee structure to create one central body with oversight authority over the disparate aspects of the issue. Without a principal point, Congress will not be able to provide effective oversight and leadership.

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 (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) * * *

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

* * * * *

TITLE II—INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION

* * * * *

Subtitle C—Information Security

* * * * *

Sec. 226. DHS cybersecurity fellows program.

* * * * *

**TITLE II—INFORMATION ANALYSIS AND
INFRASTRUCTURE PROTECTION**

* * * * *

Subtitle C—Information Security

* * * * *

SEC. 226. DHS CYBERSECURITY FELLOWS PROGRAM.(a) *ESTABLISHMENT.*—

(1) *IN GENERAL.*—The Secretary shall establish a fellowship program in accordance with this section for the purpose of bringing State, local, tribal, and private sector officials to participate in the work of the National Cybersecurity Division in order to assist with the Department's stated cybersecurity missions and capabilities, including—

(A) enhancing Federal, State, local, and tribal government cybersecurity;

(B) developing partnerships with other Federal agencies, State, local, and tribal governments, and the private sector;

(C) improving and enhancing public/private information sharing involving information regarding cyber attacks, threats, and vulnerabilities;

(D) providing and coordinating incident response and recovery planning efforts; and

(E) fostering training and certification.

(2) *PROGRAM NAME.*—The program under this section shall be known as the DHS Cybersecurity Fellows Program.

(b) *ELIGIBILITY.*—In order to be eligible for selection as a fellow under the program, an individual must—

- (1) have cybersecurity-related responsibilities;
- (2) be eligible to possess an appropriate national security clearance; and
- (3) if the individual has, or is employed by a person that has, a contract with the Department or business before the Department, report to the Secretary any conflicts of interest of the individual with respect to such contract or business.

(c) *LIMITATIONS.*—The Secretary—

- (1) may conduct up to 2 iterations of the program each year, each of which shall be 180 days in duration; and
- (2) shall ensure that the number of fellows selected for each iteration does not impede the activities of the National Cybersecurity Division.

(d) *CONDITION.*—As a condition of selecting an individual as a fellow under the program, the Secretary shall verify that the individual's employer agrees to continue to pay the individual's salary and benefits during the period of the fellowship.

(e) *STIPEND.*—During the period of the fellowship of an individual under the program, the Secretary may, subject to the availability of appropriations, provide to the individual a stipend to cover the individual's reasonable living expenses during the period of the fellowship.

* * * * *