

**DHS CYBERSECURITY ON-THE-JOB TRAINING
PROGRAM ACT**

JULY 27, 2023.—Committed to the Committee of the Whole House on the State of
the Union and ordered to be printed

**Mr. GREEN of Tennessee, from the Committee on Homeland
Security, submitted the following**

R E P O R T

[To accompany H.R. 3208]

The Committee on Homeland Security, to whom was referred the bill (H.R. 3208) to amend the Homeland Security Act of 2002 to establish a DHS Cybersecurity On-the-Job Training Program, and for other purposes, having considered the same, reports favorably thereon without amendment and recommends that the bill do pass.

CONTENTS

	Page
Purpose and Summary	1
Background and Need for Legislation	2
Hearings	2
Committee Consideration	3
Committee Votes	3
Committee Oversight Findings	3
C.B.O. Estimate, New Budget Authority, Entitlement Authority, and Tax Expenditures	3
Federal Mandates Statement	3
Duplicative Federal Programs	3
Statement of General Performance Goals and Objectives	3
Congressional Earmarks, Limited Tax Benefits, and Limited Tariff Benefits ...	4
Advisory Committee Statement	4
Applicability to Legislative Branch	4
Section-by-Section Analysis of the Legislation	4

PURPOSE AND SUMMARY

As the interconnectivity of Americans' daily lives continues to grow, the threat of malicious cyber activity has also grown. We need the right people, with the right skills, in the right jobs to confront this threat. Despite this increasingly complex threat land-

scape, some estimates say that the U.S. currently has more than 660,000 cyber job openings across the public and private sectors.¹

The Department of Homeland Security (DHS) has begun to increase its focus on closing its own cybersecurity workforce gap. Seven years after Congress gave DHS the authority, the Department launched the Cyber Talent Management System (CTMS) in November 2021. The main goals of the CTMS initiative are “to cut the time it takes to hire cybersecurity professionals, redefine how the government evaluates cybersecurity skill sets, and facilitate competitive pay rates.”² The full framework attempts to aid the agency in defining, attracting, and retaining new talent, but public reporting indicates that hiring through CTMS has been slow.

Concurrently, the Cybersecurity and Infrastructure Security Agency (CISA) was charged in the President’s Management Agenda with building a modern cyber workforce through skills training. CISA has since established the Federal Cyber Defense Skilling Academy (FCDSA) which trains current DHS employees to be entry level cyber defense analysts.³ As CTMS ramps up to hire new talent at DHS HQ, Congress must empower CISA to reskill existing DHS employees to support the Department’s vital cybersecurity mission.

H.R. 3208 solidifies CISA’s role in providing cybersecurity training to DHS employees who are not currently in cybersecurity positions. The bill formally authorizes CISA’s training activities in this space, in consultation with the Under Secretary for Management, while also giving them the flexibility needed to expand and adapt the program to address the growing cyber workforce gap.

BACKGROUND AND NEED FOR LEGISLATION

Given the number of cyber job openings across the United States, including over 45,000 of those openings within the public sector, DHS must do more to bolster its own cyber workforce and that of the federal civilian executive branch. Congress has authorized the CTMS program and appropriated millions of dollars for the Department to begin to reduce this gap. As CTMS matures, this bill will provide a near-term solution that further supports Congress’ intent to expand the Department’s cyber talent pipeline.

HEARINGS

The Committee held the following hearing in the 118th Congress that informed H.R. 3208:

On April 27, 2023, the Subcommittee on Cybersecurity and Infrastructure Protection held a hearing entitled “CISA 2025: The State of American Cybersecurity from CISA’s Perspective.” The Subcommittee received testimony from the Honorable Jen Easterly, Director, Cybersecurity and Infrastructure Security Agency.

¹ <https://www.cyberseek.org/heatmap.html>.

² <https://www.dhs.gov/news/2021/11/15/dhs-launches-innovative-hiring-program-recruit-and-retain-world-class-cyber-talent>.

³ <https://www.nist.gov/system/files/documents/2022/05/03/2022%20FEDERAL%20CYBER%20SECURITY%20WORK>.

COMMITTEE CONSIDERATION

The Committee met on Wednesday, May 17, 2023, a quorum being present, to consider H.R. 3208 and ordered the measure to be favorably reported to the House by voice vote.

COMMITTEE VOTES

Clause 3(b) of rule XIII 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. 3208.

COMMITTEE OVERSIGHT FINDINGS

In compliance with clause 3(c)(1) of rule XIII, the Committee advises that the findings and recommendations of the Committee, based on oversight activities under clause 2(b)(1) of rule X, are incorporated in the descriptive portions of this report.

CONGRESSIONAL BUDGET OFFICE ESTIMATE, NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

With respect to the requirements of clause 3(c)(2) of rule XIII and section 308(a) of the Congressional Budget Act of 1974, and with respect to the requirements of clause 3(c)(3) of rule XIII and section 402 of the Congressional Budget Act of 1974, the Committee has requested, but not received, from the Director of the Congressional Budget Office a statement as to whether this bill contains any new budget authority, spending authority, credit authority, or an increase or decrease in revenues or tax expenditures. The Committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office upon its release.

FEDERAL MANDATES STATEMENT

An estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act was not made available to the Committee in time for the filing of this report. The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office upon its release.

DUPLICATIVE FEDERAL PROGRAMS

Pursuant to clause 3(c) of rule XIII, the Committee finds that H.R. 3208 does not contain any provision that establishes or reauthorizes a program known to be duplicative of another Federal program.

STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause 3(c)(4) of rule XIII, the objective of H.R. 3208 is to establish a DHS Cybersecurity On-the-Job Training Program.

CONGRESSIONAL EARMARKS, LIMITED TAX BENEFITS, AND LIMITED TARIFF BENEFITS

In compliance with rule XXI, 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 rule XXI.

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 THE LEGISLATIVE BRANCH

The Committee finds that H.R. 3208 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 states the Act may be cited as the “DHS Cybersecurity On-the-Job Training Program Act.”

Section. 2. DHS Cybersecurity On-the-Job Training Program

This section amends the Homeland Security Act of 2002 to establish a DHS Cybersecurity On-the-Job Training Program within CISA to provide training to DHS employees not currently in a cybersecurity position for work in matters relating to cybersecurity at DHS.

This section further directs CISA to develop a curriculum for the Program, incorporating any existing curricula as appropriate, which may include distance learning, in-classroom learning, on-the-job instruction, or other means of training and education. The section requires the curriculum to be consistent with the National Initiative for Cybersecurity Education (NICE) Framework. The Committee expects CISA to utilize the most updated NICE Framework and to measure success of the Program using metrics developed in line with the framework, adjusting curriculum and trainings, as appropriate, to maximize the effectiveness of the Program.

This section also directs CISA to develop criteria for participation in the Program and to offer training in line with curriculum developed under this Act. CISA is required to provide an annual report to Congress for seven years, including information on the number of employees participating, the positions into which Program participants were hired after training, a description of metrics used to measure the success of the Program, and copies of the required report on annual cybersecurity vacancies.

This section further directs the DHS Under Secretary for Management to support the Program by submitting to the DHS Secretary an annual report on cybersecurity vacancies at DHS, identifying and recruiting individuals for the Program, implementing policies (including continuing service agreements) to encourage Program participation, and conducting outreach to Program participants on job opportunities after completing the Program.

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 italics 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:

Sec. 1. Short title; table of contents.

* * * * *

TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

* * * * *

Subtitle A—Cybersecurity and Infrastructure Security

* * * * *

Sec. 2220F. DHS Cybersecurity On-the-Job Training Program.

* * * * *

TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

* * * * *

Subtitle A—Cybersecurity and Infrastructure Security

* * * * *

SEC. 2220F. DHS CYBERSECURITY ON-THE-JOB TRAINING PROGRAM.

(a) **IN GENERAL.**—There is established within the Agency a “DHS Cybersecurity On-the-Job Training Program” (in this section referred to as the “Program”) to voluntarily train Department employees who are not currently in a cybersecurity position for work in matters relating to cybersecurity at the Department. The Program shall be led by the Director, in consultation with the Under Secretary for Management.

(b) **DUTIES OF THE DIRECTOR.**—In carrying out the Program under subsection (a), the Director—

(1) shall develop a curriculum for the Program, incorporating any existing curricula as appropriate, and consistent with the National Initiative for Cybersecurity Education Framework or any successor framework, which may include distance learning instruction, in-classroom instruction within a work location, on-the-job instruction under the supervision of experienced cybersecurity staff, or other means of training and education as determined appropriate by the Director;

(2) shall develop criteria for participation in the Program;
(3) in accordance with paragraph (1), shall provide cybersecurity training to employees of the Department and may, as appropriate, provide cybersecurity training to other Federal employees; and

(4) shall annually for seven years submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report that includes—

- (A) information relating to the number of employees who participated in the Program in the preceding year;
- (B) an identification of the positions into which employees trained through the Program were hired after such training;
- (C) a description of metrics used to measure the success of the Program;
- (D) copies of the reports submitted pursuant to (c)(1); and
- (E) any additional information relating to the duties specified in this subsection.

(c) DUTIES OF THE UNDER SECRETARY FOR MANAGEMENT.—In carrying out the Program under subsection (a), the Under Secretary for Management shall—

- (1) submit to the Secretary an annual report on the status of vacancies in cybersecurity positions throughout the Department;
- (2) support efforts by the Director to identify and recruit individuals employed by the Department to participate in the Program;
- (3) implement policies, including continuing service agreements, to encourage participation in the Program by employees throughout the Department; and
- (4) conduct outreach to employees who complete the Program regarding cybersecurity job opportunities within the Department.

* * * * *

