114TH CONGRESS
1st Session
HOUSE OF REPRESENTATIVES
REPT. 114–345
Part 1

STRENGTHENING STATE AND LOCAL CYBER CRIME FIGHTING ACT

NOVEMBER 19, 2015.—Ordered to be printed

Mr. GOODLATTE, from the Committee on the Judiciary, submitted the following

R E P O R T

[To accompany H.R. 3490]

[Including cost estimate of the Congressional Budget Office]

The Committee on the Judiciary, to whom was referred the bill (H.R. 3490) to amend the Homeland Security Act of 2002 to authorize the National Computer Forensics Institute, and for other purposes, having considered the same, reports favorably thereon with an amendment and recommends that the bill as amended do pass.

CONTENTS

The Amendment

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 "Strengthening State and Local Cyber Crime Fighting Act".

SEC. 2. AUTHORIZATION OF THE NATIONAL COMPUTER FORENSICS INSTITUTE OF THE DEPARTMENT OF HOMELAND SECURITY.

(a) IN GENERAL.—Subtitle C of title VIII of the Homeland Security Act of 2002 (6 U.S.C. 381 et seq.) is amended by adding at the end the following new section:

"SEC. 822. NATIONAL COMPUTER FORENSICS INSTITUTE.

"(a) IN GENERAL.—There is established in the Department a National Computer Forensics Institute (in this section referred to as the 'Institute'), to be operated by the United States Secret Service, for the dissemination of homeland security information related to the investigation and prevention of cyber and electronic crime and related threats to educate, train, and equip State, local, tribal, and territorial law enforcement officers, prosecutors, and judges.

"(b) FUNCTIONS.—The functions of the Institute shall include the following:

"(1) Educating State, local, tribal, and territorial law enforcement officers, prosecutors, and judges on current—

"(A) cyber and electronic crimes and related threats;

"(B) methods for investigating cyber and electronic crime and related threats and conducting computer and mobile device forensic examinations; and

"(C) prosecutorial and judicial challenges related to cyber and electronic crime and related threats, and computer and mobile device forensic examinations.

"(2) Training State, local, tribal, and territorial law enforcement officers to—

"(A) conduct cyber and electronic crime and related threat investigations;

"(B) conduct computer and mobile device forensic examinations; and

"(C) respond to network intrusion incidents.

"(3) Training State, local, tribal, and territorial law enforcement officers, prosecutors, and judges on methods to obtain, process, store, and admit digital evidence in court.

"(c) PRINCIPLES.—In carrying out the functions under subsection (b), the Institute shall ensure, to the extent practicable, that timely, actionable, and relevant expertise and homeland security information related to cyber and electronic crime and related threats is shared with State, local, tribal, and territorial law enforcement officers, prosecutors, and judges.

"(d) EQUIPMENT.—The Institute is authorized to provide State, local, tribal, and territorial law enforcement officers, prosecutors, and judges with computer equipment, hardware, software, manuals, and tools necessary to conduct cyber and electronic crime and related threats investigations and computer and mobile device forensic examinations.

"(e) ELECTRONIC CRIME TASK FORCES.—The Institute shall facilitate the expansion of the Secret Service's network of Electronic Crime Task Forces through the addition of task force officers of State, local, tribal, and territorial law enforcement officers, prosecutors, and judges educated and trained at the Institute, in addition to academia and private sector stakeholders.

"(f) COORDINATION WITH FEDERAL LAW ENFORCEMENT TRAINING CENTER.—The Institute shall seek opportunities to coordinate with the Federal Law Enforcement Training Center within the Department to help enhance, to the extent practicable, the training provided by the Center to stakeholders, including by helping to ensure that such training reflects timely, actionable, and relevant expertise in homeland security information related to cyber and electronic crime and related threats.".

(b) NO ADDITIONAL FUNDING.—No additional funds are authorized to be appropriated to carry out this Act and the amendment made by this Act. This Act and such amendment shall be carried out using amounts otherwise available for such purposes.

(c) CLERICAL AMENDMENT.—The table of contents of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 821 the following new item:

"Sec. 822. National Computer Forensics Institute.".

Purpose and Summary

This bill amends the Homeland Security Act of 2002 to establish in the Department of Homeland Security a National Computer Forensics Institute to be operated by the U.S. Secret Service for the dissemination of homeland security information related to the investigation and prevention of cyber and electronic crime, including threats or acts of terrorism, to educate, train, and equip State,

local, tribal, and territorial law enforcement officers, prosecutors, and judges.

Background and Need for the Legislation

Cyber crime is a growing threat throughout our Nation. In addition to large and sophisticated cyber schemes, a growing number of less sophisticated crimes still contain some cyber element. The National Computer Forensic Institute ("The Institute") provides much needed education and training on investigation methods, computer and mobile device forensic examinations, network intrusion incidents, and methods to obtain, process, store, and admit digital evidence in court. The Institute is responsible for the dissemination of homeland security information related to the investigation and prevention of cyber and electronic crime, education, training, and the equipping of State, local, tribal and territorial law enforcement officers, prosecutors, and judges.

This legislation originates from a program developed by the State of Alabama. In 2007, Alabama approached the Federal Government via the United States Secret Service (USSS) and the Department of Homeland Security and proposed a facility that would train State and local law enforcement, prosecutors, and judges on the intricacies of the legal issues surrounding cyber crime. Alabama came to an agreement with the Federal Government in which the State would provide the location and facility and the USSS would provide the instructors, administration, and funds to train.

Today, the Institute exists as a federally-funded training center that instructs law enforcement officials from throughout the United States on digital evidence and cyber crime investigations. The USSS's Criminal Investigative Division and the Alabama Office of Prosecution Services jointly run the 32,000 square-foot facility located in Hoover, Alabama. The curriculum for the training conducted at the facility focuses on current trends in cyber crime and is taught by the USSS. Thus far, the Institute has trained police officials and legal professionals from all 50 States and from 3 U.S. Territories. The Institute has provided critical training to the law enforcement community and has earned the reputation of the nation's "premiere hi-tech crime training facility." The Act will codify the program by officially authorizing it in law.

Alabama and other States that have sent their law enforcement personnel to the facility have seen a range of benefits from the Institute including free, advanced cyber crime education and provided-for per diem and travel costs. Additionally, the students that attend the Institute receive the same equipment and software used by the USSS. The students then return to their local institutions with the knowledge and ability to not only conduct investigations themselves, but also with the ability to train other people in their agency on cyber-protocol.

The Institute opened on May 19, 2008, and since that time has trained police officials, prosecutors, and judges from all 50 States and 3 territories from over 500 agencies throughout the Nation. The students that finish the program at the Institute leave with the ability to conduct individual cyber crime examinations, which substantially increases the operational capabilities of their respective agencies.

Hearings

The Committee on the Judiciary held no hearings on H.R. 3490.

Committee Consideration

On September 30, 2015 the Committee met in open session and ordered the bill H.R. 3490 favorably reported with an amendment, by voice vote, a quorum being present.

Committee Votes

In compliance with clause 3(b) of rule XIII of the Rules of the House of Representatives, the Committee advises that there were no recorded votes during the Committee's consideration of H.R. 3490

Committee Oversight Findings

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

New Budget Authority and Tax Expenditures

Clause 3(c)(2) of rule XIII of the Rules of the House of Representatives is inapplicable because this legislation does not provide new budgetary authority or increased tax expenditures.

Congressional Budget Office Cost Estimate

In compliance with clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, the Committee sets forth, with respect to the bill, H.R. 3490, the following estimate and comparison prepared by the Director of the Congressional Budget Office under section 402 of the Congressional Budget Act of 1974:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, October 19, 2015.

Hon. BOB GOODLATTE, CHAIRMAN,
Committee on the Judiciary,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 3490, the "Strengthening State and Local Cyber Crime Fighting Act."

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Mark Grabowicz, who can be reached at 226–2860.

Sincerely,

KEITH HALL,
DIRECTOR.

Enclosure

cc: Honorable John Conyers, Jr.
Ranking Member

H.R. 3490—Strengthening State and Local Cyber Crime Fighting Act.

As ordered reported by the House Committee on the Judiciary on September 30, 2015.

H.R. 3490 would establish in the Department of Homeland Security (DHS) a National Computer Forensics Institute to educate and train State and local law enforcement officers, prosecutors, and judges on matters relating to cyber and electronic crime and to share information with such personnel in the prevention and investigation of those crimes. The department is currently carrying out activities similar to those required by the bill, and CBO estimates that implementing H.R. 3490 would not have a significant effect on spending by DHS. Because enacting the legislation would not affect direct spending or revenues, pay-as-you-go procedures do not apply.

CBO estimates that enacting H.R. 3490 would not increase net direct spending or on-budget deficits in any of the four consecutive 10-year periods beginning in 2026.

H.R. 3490 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act.

On October 7, 2015, CBO transmitted a cost estimate for H.R. 3490 as ordered reported by the House Committee on Homeland Security on September 30, 2015. The two versions of the bill are similar and CBO's estimates of the budgetary effects are the same.

The CBO staff contact for this estimate is Mark Grabowicz. The estimate was approved by H. Samuel Papenfuss, Deputy Assistant Director for Budget Analysis.

Duplication of Federal Programs

No provision of H.R. 3490 establishes or reauthorizes a program of the Federal Government known to be duplicative of another Federal program, a program that was included in any report from the Government Accountability Office to Congress pursuant to section 21 of Public Law 111–139, or a program related to a program identified in the most recent Catalog of Federal Domestic Assistance.

Disclosure of Directed Rule Makings

The Committee estimates that H.R. 3490 specifically directs to be completed no specific rule makings within the meaning of 5 U.S.C. 551.

Performance Goals and Objectives

The Committee states that pursuant to clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, H.R. 3490, will establish a cyber training institute that will provide education to officers, judges, and prosecutors throughout the country.

Advisory on Earmarks

In accordance with clause 9 of rule XXI of the Rules of the House of Representatives, H.R. 3490 does not contain any congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9(e), 9(f), or 9(g) of Rule XXI.

Section-by-Section Analysis

Section 1. Short Title

Section 1 provides for the short title of the legislation, the "Strengthening State and Local Cyber Crime Fighting Act."

Section 2. Authorization of the National Computer Forensics Institute of the Department of Homeland Security

Subsection (a) establishes the new National Computer Forensics Institute as a department under the operation of the USSS. The subsection also sets forth the Institute's responsibility for the dissemination of homeland security information related to the investigation and prevention of cyber and electronic crime to educate, train, and equip State, local, tribal, and territorial law enforcement officers, prosecutors, and judges.

Subsection (b) provides for the functions of the Institute, which shall include the following: (1) Educating State, local, tribal and territorial law enforcement officers, prosecutors, and judges on current—(A) cyber and electronic crimes and related threats, (B) methods for investigating cyber and electronic crimes, and conducting computer and mobile device forensic examinations; and (C) prosecutorial and judicial challenges related to cyber and electronic crimes, and computer and mobile device forensic examinations; (2) Training State, local, tribal, and territorial law enforcement officers to—(A) conduct cyber and electronic crime investigations; (B) conduct computer and mobile device forensic examinations; and (C) respond to network intrusion incidents; (3) Training State, local, tribal, and territorial law enforcement officers, prosecutors, and judges on methods to obtain, process, store, and admit digital evidence in court.

Subsection (c) provides for the principles of the Institute. This subsection requires that in carrying out the functions under subsection (b), the Institute shall ensure, to the extent practicable, that timely, actionable, and relevant expertise and homeland security information related to cyber and electronic crime is shared with State, local, tribal, and territorial law enforcement officers, prosecutors, and judges.

Subsection (d) provides for the equipment available to the Institute. This subsection authorizes the Institute to provide State, local, tribal and territorial law enforcement officers, prosecutors, and judges with computer equipment, hardware, software, manuals, and tools necessary to conduct cyber and electronic crimes investigations and computer and mobile device forensic examinations.

Subsection (e) provides for the Electronic Crime Task Forces (the "ECTF"). This provision requires the Institute to facilitate the expansion of the USSS's network of ECTF through the addition of task force officers of State, local, tribal, and territorial law enforcement officers, prosecutors, and judges educated and trained at the Institute, in addition to academia and private sector stakeholders.

Subsection 2(b) of the Act provides for no additional funding. This provision sets forth that no additional funds are authorized to be appropriated to carry out the Act and the amendment made by the Act and that the Act and amendment shall be carried out using amounts otherwise available for such purposes.

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:

* * * * * * *

* * * * * * *

TITLE VIII—COORDINATION WITH NON-FEDERAL ENTITIES; INSPECTOR GENERAL; UNITED STATES SECRET SERVICE; COAST GUARD; GENERAL PROVISIONS

* * * * * * *

Subtitle C—United States Secret Service

* * * * * * *

SEC. 822. NATIONAL COMPUTER FORENSICS INSTITUTE.

(a) IN GENERAL.—There is established in the Department a National Computer Forensics Institute (in this section referred to as the "Institute"), to be operated by the United States Secret Service, for the dissemination of homeland security information related to the investigation and prevention of cyber and electronic crime and related threats to educate, train, and equip State, local, tribal, and territorial law enforcement officers, prosecutors, and judges.

(b) FUNCTIONS.—The functions of the Institute shall include the following:

(1) Educating State, local, tribal, and territorial law enforcement officers, prosecutors, and judges on current—

(A) cyber and electronic crimes and related threats;

(B) methods for investigating cyber and electronic crime and related threats and conducting computer and mobile device forensic examinations; and

(C) prosecutorial and judicial challenges related to cyber and electronic crime and related threats, and computer and mobile device forensic examinations.

(2) Training State, local, tribal, and territorial law enforcement officers to—

(A) conduct cyber and electronic crime and related threat investigations;

(B) conduct computer and mobile device forensic examinations; and

(C) respond to network intrusion incidents.

(3) Training State, local, tribal, and territorial law enforcement officers, prosecutors, and judges on methods to obtain, process, store, and admit digital evidence in court.

(c) PRINCIPLES.—In carrying out the functions under subsection (b), the Institute shall ensure, to the extent practicable, that timely, actionable, and relevant expertise and homeland security information related to cyber and electronic crime and related threats is shared with State, local, tribal, and territorial law enforcement officers, prosecutors, and judges.

(d) EQUIPMENT.—The Institute is authorized to provide State, local, tribal, and territorial law enforcement officers, prosecutors, and judges with computer equipment, hardware, software, manuals, and tools necessary to conduct cyber and electronic crime and related threats investigations and computer and mobile device forensic examinations.

(e) ELECTRONIC CRIME TASK FORCES.—The Institute shall facilitate the expansion of the Secret Service's network of Electronic Crime Task Forces through the addition of task force officers of State, local, tribal, and territorial law enforcement officers, prosecutors, and judges educated and trained at the Institute, in addition to academia and private sector stakeholders.

(f) COORDINATION WITH FEDERAL LAW ENFORCEMENT TRAINING CENTER.—The Institute shall seek opportunities to coordinate with the Federal Law Enforcement Training Center within the Department to help enhance, to the extent practicable, the training provided by the Center to stakeholders, including by helping to ensure that such training reflects timely, actionable, and relevant expertise in homeland security information related to cyber and electronic crime and related threats.

* * * * * * *

○