114TH CONGRESS
1st Session
HOUSE OF REPRESENTATIVES
REPT. 114–345
Part 2

STRENGTHENING STATE AND LOCAL CYBER CRIME FIGHTING ACT

NOVEMBER 30, 2015.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. MCCAUL, from the Committee on Homeland Security, 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 Homeland Security, 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, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

The amendment is as follows:

Strike out 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.".

SEC. 3. TRAINING MATERIALS.

Not later than six months after the date of the enactment of this Act, the Director of the United States Secret Service shall report to the appropriate congressional oversight committees on plans to incorporate best practices into training materials on chain of custody for digital evidence, including physical devices and the digital evidence that may be contained on such devices.

SEC. 4. RULE OF CONSTRUCTION.

Nothing in this Act may be construed to abridge the rights afforded by the Fourth and Fifth Amendments to the United States Constitution.

PURPOSE AND SUMMARY

H.R. 3490, the Strengthening State and Local Cyber Crime Fighting Act of 2015, codifies the National Computer Forensics Institute (NCFI), which is operated by the United States Secret Service (USSS). The NCFI provides training for State and local investigators, prosecutors, and judges on how to investigate cyber and electronic crimes, conduct computer and mobile device forensic examinations, and respond to network intrusion investigations.

This legislation would also help to facilitate the expansion of the USSS network of Electronic Crimes Task Forces (ECTF) throughout the country. The ECTF's conduct quarterly meetings of law enforcement, industry, academia, and other stakeholders to discuss trends and best practices in information security strategies and cybercrime fighting.

BACKGROUND AND NEED FOR LEGISLATION

Today's criminals present new challenges to State and local law enforcement investigators, prosecutors, and judges. Cyber criminals use technology to commit almost every type of crime. As such, it is imperative that we provide tools and training to address these challenges to law enforcement and to protect the elderly, veterans, children, small business owners, and others from being exploited through their computers, mobile devices and the Internet.

Since 2008, the USSS has operated the NCFI. Located in Hoover, Alabama, the NCFI is a 32,000 square foot facility consisting of four multi-purpose classrooms, one-network investigation classroom, a mock courtroom, administrative work areas and an operational forensics laboratory.

While NCFI has been in existence for more than 7 years, it has not yet been authorized. The NCFI has garnered a reputation as the premier cybercrime training center in the nation supporting State and local law enforcement investigators, prosecutors, and judicial officials. To date, the NCFI has trained and equipped more than 4,590 local officials from all 50 States and three U.S. Territories. These NCFI graduates represent more than 1,500 agencies Nationwide.

HEARINGS

No hearings were held on H.R. 3490, however the Committee held the following oversight hearing.

On February 12, 2015, the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies held a hearing entitled "Emerging Threats and Technologies to Protect the Homeland." The Subcommittee received testimony from Mr. Andy Ozment, Assistant Secretary, Office of Cybersecurity and Communications, National Protection and Programs Directorate, U.S. Department of Homeland Security; Dr. Huban Gowadia, Director, Domestic Nuclear Detection Office, U.S. Department of Homeland Security; Mr. Joseph Martin, Acting Director, Homeland Security Enterprise and First Responders Group, Science and Technology Di-

rectorate, U.S. Department of Homeland Security; Mr. William Noonan, Deputy Special Agent in Charge, Criminal Investigative Division, Cyber Operations Branch, United States Secret Service, U.S. Department of Homeland Security; and Mr. William Painter, Analyst, Government and Finance Division, Congressional Research Service, Library of Congress.

COMMITTEE CONSIDERATION

The Committee met on September 30, 2015, to consider H.R. 3490, and ordered the measure to be reported to the House with a favorable recommendation, as amended, by voice vote. The Committee took the following actions:

The following amendments were offered:

An Amendment in the Nature of a Substitute offered by MR. RATCLIFFE (#1); was AGREED TO by voice vote.

An Amendment by MEMBER to the Amendment in the Nature of a Substitute (#1a); was WITHDRAWN by unanimous consent.

An en bloc amendment to the Amendment in the Nature of a Substitute offered by MS. JACKSON LEE (#1A); was AGREED TO by voice vote.

Consisting of the following amendments:
Add at the end of the bill a new section entitled "Sec. 3. Training Materials."

Add at the end of the bill a new section entitled "Sec. 3. Rule of Construction."

The Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies met on September 17, 2015, to consider H.R. 3490 and reported the measure to the Full Committee with a favorable recommendation, as amended, by voice vote.

The following amendment was offered:

An Amendment offered by MR. RICHMOND (#1); was AGREED TO by voice vote.

Page 4, line 16, strike the closing quotation marks and the second period.
Page 4, beginning line 17, insert a new section entitled "(f) Coordination With Federal Law Enforcement Training Center."

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 consideration of H.R. 3490.

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. 3490, the Strengthening State and Local Cyber Crime Fighting Act, 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.

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. 3490 contains the following general performance goals and objectives, including outcome related goals and objectives authorized.

The goals of this legislation include:

- Enhancing the capabilities of State, local, Tribal and territorial law enforcement, prosecutors and judges to investigate and prosecute crimes involving cyber and electronic crimes.
- Training State, local, Tribal and territorial law enforcement officers to conduct cybercrime investigations, computer and mobile device forensics and respond to network intrusions.
- Training State, local, Tribal and territorial law enforcement, prosecutors and judges on methods to obtain, process, store and admit digital evidence in court.
- Ensuring the information shared with State, local, Tribal and territorial law enforcement, prosecutors and judges is timely, actionable and relevant homeland security information related to cyber and electronic crimes.

DUPLICATIVE FEDERAL PROGRAMS

Pursuant to clause 3(c) of rule XIII, the Committee finds that H.R. 3490 does not contain any provision that establishes or reauthorizes a program known to be duplicative of another Federal program.

This legislation does not establish a new program. However the Committee notes that the National Computer Forensic Institute is operated by the United States Secret Service and is codified through this legislation.

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

PREEMPTION CLARIFICATION

In compliance with section 423 of the Congressional Budget Act of 1974, requiring the report of any Committee on a bill or joint resolution to include a statement on the extent to which the bill or joint resolution is intended to preempt State, local, or Tribal law, the Committee finds that H.R. 3490 does not preempt any State, local, or Tribal law.

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, October 7, 2015.

Hon. MICHAEL MCCAUL,
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. 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.

Sincerely,

KEITH HALL.

Enclosure.

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

H.R. 3490 would establish in the Department of Homeland Security 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 significantly affect spending by DHS. Because enacting the legislation would not affect direct spending or revenues, pay-as-you-go procedures do not apply.

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

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

DISCLOSURE OF DIRECTED RULE MAKINGS

The Committee estimates that H.R. 3490 would require no directed rule makings.

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 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 provides that bill 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.

Subtitle C of title VII of the Homeland Security Act of 2002 is amended to add a new Section 822.

"SEC. 822. NATIONAL COMPUTER FORENSICS INSTITUTE.

This subsection establishes within the Department a National Computer Forensics Institute to be operated by the United States Secret Service.

(b) Functions.

This subsection establishes the functions of the institute. The functions shall include: Educating State, local, Tribal and territorial law enforcement, prosecutors and judges on cyber and electronic crimes and threats; methods for investigating cyber and electronic crimes; and prosecutorial and judicial challenges related to cyber and electronic crimes.

This subsection also requires the Institute to train State, local, Tribal and territorial law enforcement officers to conduct cybercrime investigations, carry out computer and mobile device forensics, and respond to network intrusions.

Finally, this subsection requires the institute to train State, local, Tribal and territorial law enforcement, prosecutors, and judges on methods to obtain, process, store and admit digital evidence in court.

(c) Principles.

This subsection requires the Institute to ensure that timely, actionable and relevant homeland security information related to cyber and electronic crime is shared with State, local, Tribal and territorial law enforcement, prosecutors, and judges.

(d) Equipment.

This subsection authorizes the transfer of computer equipment and supporting tools to State, local, Tribal and territorial law enforcement, prosecutors and judges.

(e) Electronic Crimes Task Forces.

This subsection recognizes the Institute's training to help facilitate membership and association with the USSS' network of ECTF's throughout the country (ECTFs conduct quarterly meetings with private industry, law enforcement, academia, and other stakeholders to discuss trends in cybercrime and best practices for information security resiliency).

(f) Coordination with Federal Law Enforcement Training Center.

This section requires the Institute to seek opportunities to coordinate with the Federal Law Enforcement Training Center (FLETC)

to help enhance training of stakeholders and ensure the training reflects timely, actionable and relevant expertise in homeland security information related to cyber and electronic crimes.

The Committee understands the inherent differences of both NCFI and FLETC, but both programs should, when appropriate, seek opportunities to share best practices in conducting cyber crime, forensics, and related training.

(b) No Additional Funding.

This subsection prohibits the authorization of additional appropriations for this program, the Director shall use existing, appropriated, funds.

(c) Clerical Amendment.

This subsection amends the table of contents of the Homeland Security Act of 2002.

Sec. 3. Training Materials.

This section requires the Director of the USSS to report to Congress on plans to incorporate best practices into training materials on chain of custody for digital evidence.

Sec. 4. Rule of Construction.

This section states that nothing in this act may be construed to abridge the rights afforded by the Fourth and Fifth Amendments to the United States Constitution.

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) 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.

* * * * * * *

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.

* * * * * * *

○