115TH CONGRESS
1st Session
HOUSE OF REPRESENTATIVES
REPORT
115–376

NIST CYBERSECURITY FRAMEWORK, ASSESSMENT, AND AUDITING ACT OF 2017

OCTOBER 31, 2017.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. SMITH of Texas, from the Committee on Science, Space, and Technology, submitted the following

R E P O R T

together with

MINORITY VIEWS

[To accompany H.R. 1224]

[Including cost estimate of the Congressional Budget Office]

The Committee on Science, Space, and Technology, to whom was referred the bill (H.R. 1224) to amend the National Institute of Standards and Technology Act to implement a framework, assessment, and audits for improving United States cybersecurity, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

79–006

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 "NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017".

SEC. 2. NIST MISSION TO ADDRESS CYBERSECURITY THREATS.

Section 20(a)(1) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(a)(1)) is amended by inserting ", emphasizing the principle that expanding cybersecurity threats require engineering security from the beginning of an information system's life cycle, building more trustworthy and secure components and systems from the start, and applying well-defined security design principles throughout" before the semicolon.

SEC. 3. IMPLEMENTATION OF CYBERSECURITY FRAMEWORK.

The National Institute of Standards and Technology Act (15 U.S.C. 271 et seq.) is amended by inserting after section 20 the following:

"SEC. 20A. FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY.

"(a) IMPLEMENTATION BY FEDERAL AGENCIES.—The Institute shall promote the implementation by Federal agencies of the Framework for Improving Critical Infrastructure Cybersecurity (in this section and section 20B referred to as the 'Framework') by providing to the Office of Management and Budget, the Office of Science and Technology Policy, and all other Federal agencies, not later than 6 months after the date of enactment of the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017, guidance that Federal agencies may use to incorporate the Framework into their information security risk management efforts, including practices related to compliance with chapter 35 of title 44, United States Code, and any other applicable Federal law.

"(b) GUIDANCE.—The guidance required under subsection (a) shall—

"(1) describe how the Framework aligns with or augments existing agency practices related to compliance with chapter 35 of title 44, United States Code, and any other applicable Federal law;

"(2) identify any areas of conflict or overlap between the Framework and existing cybersecurity requirements, including gap areas where additional policies, standards, guidelines, or programs may be needed to encourage Federal agencies to use the Framework and improve the ability of Federal agencies to manage cybersecurity risk;

"(3) include a template for Federal agencies on how to use the Framework, and recommend procedures for streamlining and harmonizing existing and future cybersecurity-related requirements, in support of the goal of using the Framework to supplant Federal agency practices in compliance with chapter 35 of title 44, United States Code;

"(4) recommend other procedures for compliance with cybersecurity reporting, oversight, and policy review and creation requirements under such chapter 35 and any other applicable Federal law; and

"(5) be updated, as the Institute considers necessary, to reflect what the Institute learns from ongoing research, the audits conducted pursuant to section 20B(c), the information compiled by the Federal working group established pursuant to subsection (c), and the annual reports published pursuant to subsection (d).

"(c) FEDERAL WORKING GROUP.—Not later than 3 months after the date of enactment of the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017, the Institute shall establish and chair a working group (in this section referred to as the 'Federal working group'), including representatives of the Office of Management and Budget, the Office of Science and Technology Policy, and other appropriate Federal agencies, which shall—

"(1) not later than 6 months after the date of enactment of the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017, develop outcome-based and quantifiable metrics to help Federal agencies in their analysis and assessment of the effectiveness of the Framework in protecting their information and information systems;

"(2) update such metrics as the Federal working group considers necessary;

"(3) compile information from Federal agencies on their use of the Framework and the results of the analysis and assessment described in paragraph (1); and

"(4) assist the Office of Management and Budget and the Office of Science and Technology Policy in publishing the annual report required under subsection (d).

"(d) REPORT.—The Office of Management and Budget and the Office of Science and Technology Policy shall develop and make publicly available an annual report on agency adoption rates and the effectiveness of the Framework. In preparing such report, the Offices shall use the information compiled by the Federal working group pursuant to subsection (c)(3).

"SEC. 20B. CYBERSECURITY AUDITS.

"(a) INITIAL ASSESSMENT.—

"(1) REQUIREMENT.—Not later than 6 months after the date of enactment of the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017, the Institute shall complete an initial assessment of the cybersecurity preparedness of the agencies described in paragraph (2). Such assessment shall be based on information security standards developed under section 20, and may also be informed by work done or reports published by other Federal agencies or officials.

"(2) AGENCIES.—The agencies referred to in paragraph (1) are the agencies referred to in section 901(b) of title 31, United States Code, and any other agency that has reported a major incident (as defined in the Office of Management and Budget Memorandum—16—03, published on October 30, 2015, or any successor document).

"(3) NATIONAL SECURITY SYSTEMS.—The requirement under paragraph (1) shall not apply to national security systems (as defined in section 3552(b) of title 44, United States Code).

"(b) AUDIT PLAN.—Not later than 6 months after the date of enactment of this Act, the Institute shall prepare a needs-based plan for carrying out the audits of agencies as required under subsection (c). Such plan shall include a description of staffing plans, workforce capabilities, methods for conducting such audits, coordination with agencies to support such audits, expected timeframes for the completion of audits, and other information the Institute considers relevant. The plan shall be transmitted by the Institute to the congressional entities described in subsection (c)(4)(F).

"(c) AUDITS.—

"(1) REQUIREMENT.—Not later than 6 months after the date of enactment of the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017, the Institute shall initiate an individual cybersecurity audit of each agency described in subsection (a)(2), to assess the extent to which the agency is meeting the information security standards developed under section 20.

"(2) RELATION TO FRAMEWORK.—Audits conducted under this subsection shall—

"(A) to the extent applicable and available, be informed by the report on agency adoption rates and the effectiveness of the Framework described in section 20A(d); and

"(B) if the agency is required by law or executive order to adopt the Framework, be based on the guidance described in section 20A(b) and metrics developed under section 20A(c)(1).

"(3) SCHEDULE.—The Institute shall establish a schedule for completion of audits under this subsection to ensure that—

"(A) audits of agencies whose information security risk is high, based on the assessment conducted under subsection (a), are completed not later than 1 year after the date of enactment of the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017, and are audited annually thereafter; and

"(B) audits of all other agencies described in subsection (a)(2) are completed not later than 2 years after the date of enactment of the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017, and are audited biennially thereafter.

"(4) REPORT.—A report of each audit conducted under this subsection shall be transmitted by the Institute to—

"(A) the Office of Management and Budget;

"(B) the Office of Science and Technology Policy;

"(C) the Government Accountability Office;

"(D) the agency being audited;

"(E) the Inspector General of such agency, if there is one; and

"(F) Congress, including the Committee on Science, Space, and Technology of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate.".

COMMITTEE STATEMENT AND VIEWS

PURPOSE AND SUMMARY

H.R. 1224, the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017, implements key ideas to help strengthen Federal government cybersecurity. The bill promotes the federal use of the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, and establishes a federal working group to develop quantifiable metrics to compile information about the effectiveness of the NIST Cybersecurity Framework in protecting federal information and information systems.

H.R. 1224 also directs NIST to complete an initial assessment of the cybersecurity preparedness of priority federal agencies and prepare a needs-based audit plan in advance of carrying out individual cybersecurity audits of each federal agency to determine the extent to which each agency is meeting the information security standards developed by NIST.

H.R. 1224 further directs NIST to establish a schedule such that agencies are either audited annually or biennially depending on their information security risk. H.R. 1224 requires a report of each audit to be submitted to the Office of Management and Budget (OMB), the Office of Science and Technology Policy (OSTP), the U.S. Government Accountability Office (GAO), the agency being audited, the agency's Office of Inspector General if it has one, and Congress, including the House Science, Space, and Technology Committee and the Senate Committee on Commerce, Science, and Transportation.

BACKGROUND AND NEED FOR LEGISLATION

This legislation stems from urgent need. The status quo of U.S. Government cybersecurity is demonstrably inadequate and growing worse. The national and economic security of the United States, and the security of Americans' personally identifiable information (PII)—held in trust by various federal departments and agencies—have been threatened by persistent cyberattacks. As the sophistication and frequency of cyberattacks by nation-states and nefarious cyber actors increases, so too does the threat to our economy, critical and virtual infrastructure, and national security.

The Trump administration has taken concrete, positive steps, notably the May 11, 2017 presidential executive order (Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure) that mandates use of the highest standard of cybersecurity risk management and imposes accountability on responsible federal agency leaders. But administrative changes alone will not suffice. Instead, Congress must take aggressive actions to support and assure a fundamentally different approach to cybersecurity that addresses the magnitude and nature of growing threats.

Just a few weeks ago, Congress learned about a multi-year cybersecurity breach at the Securities and Exchange Commission (SEC). Federal investigators believe they have shut down the breach, but it will be months or even years before there is a complete accounting of illicit profits reaped by foreign cyber-criminals through theft of confidential financial information from the SEC.

On October 25, 2017, the Committee held an investigative hearing about the infiltration of Kaspersky Lab into U.S. Government computer systems. Kaspersky Lab is a Moscow-headquartered cybersecurity operation, founded by a former Russian cyberwarfare specialist. After discovering close links between Kaspersky Lab and the Russian government and its intelligence apparatus, U.S. national security agencies expressed concern with the presence and use of Kaspersky Lab products and services on federal information systems.

Several federal civilian agencies, however, either disregarded or were unaware of Kaspersky Lab's provenance and the risks of embedding Kaspersky Lab software on U.S. Government computer systems. As a result, agencies engaged Kaspersky Lab as an approved U.S. Government contractor and purchased Kaspersky Lab cybersecurity products and services.

The consequences of these foolhardy decisions are still not fully understood, but the nature and seriousness of the risks were verified when the Israeli intelligence service shared with its U.S. counterparts evidence that Kaspersky Lab cybersecurity software embedded in agency and contractor computer systems had enabled extraction of sensitive U.S. national security information—which was, not surprisingly, forwarded to Moscow. After the fact, the U.S. Department of Homeland Security (DHS) reacted by directing all federal agencies to begin removing Kaspersky Lab software within 90 days. As this purge of Kaspersky Lab software continues, however, federal investigators are trying to determine how much sensitive information was taken by Kaspersky Lab and passed along to the Russian government.

These recent incidents are not isolated occurrences. Scarcely a month goes by without news that cyber-criminals—independent or, more often, sponsored by unfriendly nations—have successfully breached federal computer systems and made off with huge troves of sensitive government information and millions of Americans' PII.

During the 114th and 115th Congresses, the Committee has held more than a dozen hearings that examined electronic data breaches at federal agencies. Cyber-criminals and adversarial nations have repeatedly attacked the computer systems of major federal agencies.

Information security incidents reported by federal agencies have jumped from 5,000 in fiscal year 2006 to 77,000 in fiscal year 2015—an increase of 1,300%. Even worse, a series of in-depth reports show that federal agencies have not responded adequately. In February, the Director of Information Security Issues at the Government Accountability Office (GAO) testified at a Research and Technology Subcommittee hearing that GAO has made more than 2,500 recommendations for improving agencies' cybersecurity regimes, but that approximately 1,000 of these remain unimplemented.

Committee hearings included detailed examinations of data breaches at several federal agencies, including the Office of Personnel Management (OPM), the Internal Revenue Service (IRS), the Department of Health and Human Services (via Healthcare.gov), and the Federal Deposit Insurance Corporation (FDIC), among others.

In 2015, OPM revealed that hackers had stolen the personnel records—including top-secret clearance files—of more than 20 million current and former federal employees. The FBI subsequently concluded that the Chinese government had sponsored this cyberattack. The full scope of the damage done by this cyberattack may not be known for years to come, but earlier this year GAO reported that OPM had failed to take necessary steps to reduce the risks of further cyberattacks.

The IRS is a consistent target for foreign cyber criminals. In 2015 and 2016, for instance, the IRS revealed that more than 700,000 taxpayers had sensitive data (e.g., Social Security numbers, dates of birth and addresses) stolen through its websites. This stolen data enabled hackers to access information from prior tax returns, which in turn allowed them to file new, fraudulent tax returns. Earlier this year, the IRS reported that a financial aid tool to help college students was used by hackers to steal $30 million from the U.S. government, leaving nearly 100,000 people at risk for identity theft. Identity theft via the IRS computer systems, and problems with timely detection and adequate response to such incidents, must be addressed creatively and immediately.

The federal government's cybersecurity status quo is, by any measure, demonstrably unacceptable. In spite of early administrative intercessions by the current Administration, cybersecurity incidents are likely to continue without dramatic change and new outside-the-box thinking. Federal agencies are generally out of compliance with statutory requirements that they meet minimum cybersecurity, technical, and risk-management standards.

Under the Federal Information Security Management Act (FISMA), the National Institute of Standards and Technology (NIST) is charged by Congress with creating and maintaining responsible cybersecurity standards for federal agencies to follow. NIST continues to do an excellent job in carrying out this mission. Its cybersecurity technical standards and risk management framework are widely regarded as among the best and most comprehensive in the world.

NIST, however, has no authority to require federal agencies to meet these standards. Under FISMA, OMB is responsible for assuring federal agency compliance. OMB, however, lacks internal cybersecurity expertise and only asks agencies to self-certify cybercompliance.

DHS also has a certain, limited responsibility for assuring federal agencies' compliance with cybersecurity standards. DHS, however, lacks authority to impose auditing of federal agencies' compliance. DHS also lacks internal expertise for evaluating agencies' cybersecurity regimes and is necessarily preoccupied with border control and nuclear, biological, chemical, explosives and other serious kinetic security threats.

Inspectors General (IGs) are a better resource for regularly assessing the compliance and sufficiency of federal agencies' cybersecurity defenses. Under FISMA, the IGs already perform annual audits of all major aspects of agencies' operations. The IGs also have statutory authority to compel agencies to produce needed information and to comply with indicated improvement and remedial actions.

What the IGs lack is crucial internal expertise for assessing cybersecurity issues. H.R. 1224, however, takes advantage of NIST's singular cybersecurity expertise. As originally reported by the Committee, H.R. 1224 would have directed NIST to conduct separate annual cybersecurity audits of federal agencies. After subsequent discussions with the Committee on Oversight and Government Reform, however, agreement was reached on a better approach that is reflected in the legislation to be considered by the full House.

H.R. 1224, as revised, places responsibility for carrying out and following up on annual cybersecurity audits of federal agencies with the IGs. Under the revised legislation, the IGs will closely consult and coordinate with NIST and rely on its singular expertise to evaluate agencies' compliance (i.e., compliance with the technical and risk management standards put forward by NIST pursuant to FISMA).

As improved, H.R. 1224 retains the essential element of annual, comprehensive auditing of federal agencies' cybersecurity compliance. Rather than directly placing NIST in an auditing and enforcement role, however, H.R. 1224 reaffirms the auditing and oversight authority of the IGs. Additionally, H.R. 1224 assures that IGs will have the benefit of the singular expertise of NIST experts—global leaders in cybersecurity research, evaluation, and the promulgation of standards—in evaluating agencies' cybersecurity compliance and recommending corrective actions.

Cyberattacks by criminals and adversarial foreign governments will continue for years to come. Unless Congress takes new steps, more of these attacks will be successful, and Americans' personal confidential information and the U.S. Government's national and economic security secrets will continue to be stolen with impunity.

H.R. 1224 leverages the existing authorities, as well as the unique expertise of agency IGs and NIST, to ensure that the status quo—inexplicable and permanently damaging passivity in the face of criminal and warlike cyber aggression—is addressed. H.R. 1244 is a real solution, not a retreat into more infighting over bureaucratic turf, and must be adopted to further bolster and fortify the cybersecurity posture of the United States.

LEGISLATIVE HISTORY

On February 27, 2017, Rep. Ralph Abraham (R–LA) introduced H.R. 1224, the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017, cosponsored by Representatives Lamar Smith (R–TX), Frank Lucas (R–OK), Barbara Comstock (R–VA) and Stephen Knight (R–CA). Amendments offered by Representatives Lamar Smith (R–TX), Ralph Abraham (R–LA) and Daniel Lipinski (D–IL), were approved by voice vote. An amendment offered by Representative Bill Foster (D–IL) was offered and withdrawn. More information on the amendments is available below. H.R. 1224 was approved by the House Science Committee by a recorded vote of 19 to 14 with 18 Republicans and one Democrat voting "YES" and 14 Democrats voting "NO".

Additionally, prior to the Committee's markup of H.R. 1224, the Committee held more than a dozen hearings related to federal cybersecurity policy, concerns and oversight over the course of the 114th Congress and into this year. These hearings were invaluable

to the development of the bill. Information on the following hearings is available on the Committee's website:

February 14, 2017, "Strengthening U.S. Cybersecurity Capabilities"

September 13, 2016, "Protecting the 2016 Elections from Cyber and Voting Machine Attacks"

July 14, 2016, "Evaluating FDIC's Response to Major Data Breaches: Is the FDIC Safeguarding Consumers' Banking Information?"

May 12, 2016, "FDIC Data Breaches: Can Americans Trust that Their Private Banking Information is Secure?"

April 14, 2016, "Can the IRS Protect Taxpayers' Personal Information?"

March 22, 2016, "An Overview of the Budget Proposal for the National Science Foundation for Fiscal Year 2017"

March 16, 2016, "An Overview of the Budget Proposal for the National Institute of Standards and Technology for Fiscal Year 2017"

March 2, 2016, "Smart Health: Empowering the Future of Mobile Apps"

January 8, 2016, "Cybersecurity: What the Federal Government Can Learn from the Private Sector"

October 28, 2015, "A Review of the Networking and Information Technology Research and Development (NITRD) Program"

October 21, 2015, "Cybersecurity for Power Systems"

July 8, 2015, "Is the OPM Data Breach the Tip of the Iceberg?"

February 26, 2015, "An Overview of the Budget Proposals for the National Science Foundation and National Institute of Standards and Technology for Fiscal Year 2016"

February 12, 2015, "Can Americans Trust the Privacy and Security of their Information on HealthCare.gov?"

January 27, 2015, "The Expanding Cyber Threat"

COMMITTEE VIEWS

In the months following the Committee's March 1, 2017 approval of H.R. 1224, the Committee has worked closely with the House Oversight and Government Reform Committee to modify the bill to make it stronger, more effective, and much less costly. The Committees have drafted alternative language that strikes the NIST requirement to plan and conduct individual cybersecurity audits of each of the 24 CFO Act federal agencies and any other agency that has reported a major incident, which had been included in H.R. 1224 as ordered reported. Instead, the revised language directs NIST to work with agency Inspectors General (IG) by providing technical assistance and other expert input in support of the annual evaluations the IGs are currently required to perform under law. The new language also requires these evaluations to include an audit or other analytical examination to be conducted by the IGs—not NIST—but with determinations and recommendations suggested by NIST included.

Striking the requirement to have NIST conduct individual agency cybersecurity audits addresses concerns from stakeholders that NIST maintain its current open relationships with agencies. Some of these concerns were identified by the Heritage Foundation in a July 2017 Issue Brief. The brief described three concerns: NIST's

lack of experience in conducting audits; chilled relationships between federal agencies and NIST (if NIST took on a perceived oversight role through direct agency audits); and the addition of another agency and congressional overseer on cybersecurity issues.

To address those and similar concerns, the Science and Oversight and Government Reform Committees have revised the ordered reported version of H.R. 1224 and produced a consensus bill. The revised language does not require NIST to conduct audits of agencies, but instead directs the Institute to work with the IGs as described above. There is no oversight role assigned to NIST and there is no additional congressional overseer on cybersecurity issues. The House Science Committee's long-standing jurisdiction over NIST already provides it oversight authority since NIST is required by law to develop standards and guidelines that federal agencies must implement to protect their information and information systems.

The revised language would also negate the current CBO cost estimate of $48 million over the 2018–2022 fiscal year period based on the bill as reported. Under the revised version, NIST does not conduct separate individual audits of federal agencies, the main cost driver identified by CBO.

Additionally, the revised bill directly addresses the concerns stated by the Committee minority while effectively elevating NIST's contributions to make possible positive, constructive impact on the current cybersecurity crisis in federal IT systems, operations, and personal privacy protection. Any remaining concerns would appear to be purely bureaucratic.

As revised, H.R. 1224 provides the federal government with the best possible tools to protect the private information of our citizens and federal agencies by finding and exposing gaps and closing vulnerabilities. It combines NIST's cybersecurity knowledge and expertise as the agency that develops technical standards and guidelines with the special investigative capabilities of agency Inspectors General. NIST would not regulate or enforce anything. H.R. 1224 also does not affect the Department of Homeland Security's authorities or programs in any way.

SECTION-BY-SECTION

Section 1. Short title

This section establishes the short title of the bill as the "NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017."

Section 2. NIST mission to address cybersecurity threats

This section amends NIST's mission under the Computer Standards Program (15 U.S.C. 278g–3(a)(1)). It directs the Institute to emphasize the principle that expanding cybersecurity threats require the engineering of security from the beginning of an information system's life cycle through building more trustworthy and secure components, and by applying well-defined security design principles throughout the system's life span.

Section 3. Implementation of cybersecurity Framework

This section creates two new sections in the NIST statute:

Sec. 20A—Framework for improving critical infrastructure cybersecurity (Framework):

Implementation and Guidance—Promotes the implementation of the Framework by having NIST provide guidance that federal agencies may use to incorporate the Framework into their information security risk management efforts, including compliance with the Federal Information Security Management Act (44 U.S.C. 35), and any other applicable Federal law. The guidance shall be provided to OMB, OSTP, and all other federal agencies within six months of the bill's enactment, and then updated as necessary.

Federal Working Group—Creates a federal working group, established and chaired by NIST, to develop outcome-based and quantifiable metrics, updated as necessary, to help federal agencies analyze and assess the effectiveness of the Framework in protecting their information and information systems. The federal working group shall be established within three months of the bill's enactment, and the metrics not later than six months after the bill's enactment. The federal working group shall also compile information from federal agencies on their use of the Framework and results of their analysis and assessment, which shall be published in an annual report by OMB and OSTP.

Sec. 20B. Cybersecurity audits:

Assessment—Directs NIST to complete an initial assessment of the cybersecurity preparedness of the 24 CFO–Act federal agencies, and any other federal agencies that have reported a major cybersecurity incident, based on the information security standards developed by NIST, not later than six months after the bill's enactment into law. This assessment may also be informed by work done or reports published by other federal agencies or officials.

Audit Plan—Not later than six months after the bill's enactment into law, directs NIST to prepare a needs-based plan for carrying out the audits described below.

Audits—Not later than six months after the bill's enactment into law, directs the Institute to initiate individual cybersecurity audits of each agency covered under the initial group assessment to determine the extent to which each agency is meeting the information security standards developed by the Institute.

Schedule—Directs NIST to establish a schedule for these audits based on the initial assessment. Agencies whose information security risk is high, shall have audits completed not later than one year after the bill's enactment into law, and then annually thereafter. Agencies that do not fall into this category shall have the initial audit completed no later than two years after the bill's enactment, and then biennially thereafter.

Relation to Framework—If Federal agencies are required by law or Executive Order to implement the Framework, then the NIST audits of each agency shall be based on the guidance it provides to agencies (described above) and the metrics developed by the Federal working group (described above).

Audit Report—A report of each Federal agency audit shall be transmitted to OMB, OSTP, GAO, the agency being audited, the agency's Office of Inspector General if it has one, and Congress, including the House Science, Space, and Technology Committee and the Senate Committee on Commerce, Science, and Transportation.

EXPLANATION OF AMENDMENTS

An amendment offered by Representative Lamar Smith (R–TX) was approved by voice vote. The Smith amendment added OMB to the federal working group established and chaired by NIST, and specified the involvement of OMB in developing and publishing the annual report based on information compiled by the federal working group.

An amendment offered by the bill's sponsor, Representative Ralph Abraham (R–LA), was approved by voice vote. The Abraham amendment struck the provision in H.R. 1224 as introduced relating to a public-private working group, along with any references to it and the report required of it.

An amendment offered by Representative Daniel Lipinski (D–IL) was approved by voice vote. The Lipinski amendment required NIST to prepare a needs-based plan for carrying out the agency audits within six months of the bill's enactment.

An amendment introduced by Representative Bill Foster (D–IL) was offered and withdrawn.

COMMITTEE CONSIDERATION

On March 1, 2017, the Committee met in open session and ordered reported favorably the bill, H.R. 1224, as amended, by roll call vote, a quorum being present.

ROLL CALL VOTES

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY - 115th

Full Committee Roll Call

Working Quorum: 13 Reporting Quorum: 20

DATE: 3/1/17

Bill: H.R. 1224 Final Passage

MEMBER	AYE	NO	PRESENT	NOT VOTING
1 Mr. SMITH, *Chair* - *TX*	X			
2 Mr. LUCAS – *OK* **	X			
3 Mr. ROHRABACHER – *CA*	X			
4 Mr. BROOKS – *AL*	X			
5 Mr. HULTGREN – *IL*	X			
6 Mr. POSEY – *FL*	X			
7 Mr. MASSIE – *KY*	X			
8 Mr. BRIDENSTINE – *OK*				
9 Mr. WEBER – *TX*	X			
10 Mr. KNIGHT – *CA*	X			
11 Mr. BABIN – *TX*	X			
12 Mrs. COMSTOCK – *VA*	X			
13 Mr. PALMER – *AL*				
14 Mr. LOUDERMILK – *GA*	X			
15 Mr. ABRAHAM – *LA*	X			
16 Mr. LAHOOD – *IL*	X			
17 Mr. WEBSTER – *FL*				
18 Mr. BANKS – *IN*	X			
19 Mr. BIGGS – *AZ*				
20 Mr. MARSHALL – *KS*	X			
21 Mr. DUNN – *FL*	X			
22 Mr. HIGGINS – *LA*	X			
1 Ms. JOHNSON, *Ranking* - *TX*		X		
2 Ms. LOFGREN –*CA*				
3 Mr. LIPINSKI – *IL*	X			
4 Ms. BONAMICI – *OR*		X		
5 Mr. BERA – *CA*		X		
6 Ms. ESTY – *CT*		X		
7 Mr. VEASEY – *TX*		X		
8 Mr. BEYER – *VA*		X		
9 Ms. ROSEN – *NV*		X		
10 Mr. MCNERNEY – *CA*		X		
11 Mr. PERLMUTTER – *CO*		X		
12 Mr. TONKO – *NY*		X		
13 Mr. FOSTER – *IL*		X		
14 Mr. TAKANO – *CA*		X		
15 Ms. HANABUSA – *HI*		X		
16 Mr. CRIST – *FL*		X		
17 VACANT				
TOTALS				

** Vice Chair

CORRESPONDENCE

TREY GOWDY, SOUTH CAROLINA
CHAIRMAN

ONE HUNDRED FIFTEENTH CONGRESS

ELIJAH E. CUMMINGS, MARYLAND
RANKING MINORITY MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143
MAJORITY (202) 225-5074
MINORITY (202) 225-5051
http://oversight.house.gov

September 19, 2017

The Honorable Lamar Smith
Chairman, Committee on Science,
Space, and Technology
U.S. House of Representatives

Dear Mr. Chairman:

I am writing concerning the jurisdictional interest of the Committee on Oversight and Government Reform in H.R. 1224, the "NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017." As a result of your having consulted with me concerning the provisions of the bill that fall within our Rule X jurisdiction, the Committee on Oversight and Government Reform will withdraw its request for a sequential referral and agrees to forego action on the bill.

The Committee takes this action with our mutual understanding that by foregoing consideration of H.R. 1224 at this time we do not waive any jurisdiction over the subject matter contained in this or similar legislation. Further, I request your support for the appointment of conferees from the Committee on Oversight and Government Reform during any House-Senate conference convened on this or related legislation.

Finally, I would ask that a copy of our exchange of letters on this matter be included in the bill report filed by the Committee on Science, Space, and Technology, as well as in the Congressional Record during floor consideration, to memorialize our understanding.

Sincerely,

Trey Gowdy

cc: The Honorable Paul D. Ryan, Speaker

The Honorable Elijah E. Cummings, Ranking Member
Committee on Oversight and Government Reform

The Honorable Eddie Bernice Johnson, Ranking Member
Committee on Science, Space, and Technology

The Honorable Thomas J. Wickham, Parliamentarian

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6301
(202) 225–6371
www.science.house.gov

September 19, 2017

The Honorable Trey Gowdy
Chairman
Committee on Oversight and Government Reform
2157 Rayburn House Office Building
Washington, D.C. 20515

Dear Mr. Chairman:

Thank you for your letter regarding the Committee on Oversight and Government Reform's jurisdictional interest in H.R. 1224, the "NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017," and your willingness to forego consideration of H.R. 1224 by your committee.

I agree that the Committee on Oversight and Government Reform has a valid jurisdictional interest in certain provisions of H.R. 1224, and that the Committee's jurisdiction will not be adversely affected by your decision to forego consideration of H.R. 1224. As you have requested, I will support your request for an appropriate appointment of outside conferees from your Committee in the event of a House-Senate conference on this or similar legislation should such a conference be convened. I especially appreciate your cooperation and input in drafting compromise legislation, and your support for the bill.

Finally, I will include a copy of your letter and this response in the *Congressional Record* during the floor consideration of this bill. Thank you again for your cooperation.

Sincerely,

Lamar Smith
Chairman

cc: The Honorable Paul Ryan
The Honorable Eddie Bernice Johnson
The Honorable Elijah Cummings
Mr. Tom Wickham, Parliamentarian

APPLICATION OF LAW TO THE LEGISLATIVE BRANCH

Section 102(b)(3) of Public Law 104–1 requires a description of the application of this bill to the legislative branch where the bill relates to the terms and conditions of employment or access to public services and accommodations. This bill promotes the federal use of the NIST Framework for Improving Critical Infrastructure Cybersecurity, and establishes a federal working group to develop quantifiable metrics to compile information about the effectiveness of the NIST Cybersecurity Framework in protecting federal information and information systems. As such this bill does not relate to employment or access to public services and accommodations.

STATEMENT OF OVERSIGHT FINDINGS AND RECOMMENDATIONS OF THE COMMITTEE

In compliance with clause 3(c)(1) of rule XIII and clause (2)(b)(1) of rule X of the Rules of the House of Representatives, the Committee's oversight findings and recommendations are reflected in the descriptive portions of this report.

STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

H.R. 1224, the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017, would promote the federal use of the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, and establish a federal working group to develop quantifiable metrics to compile information about the effectiveness of the NIST Cybersecurity Framework in protecting federal information and information systems.

DUPLICATION OF FEDERAL PROGRAMS

No provision of H.R. 1224 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 enacting H.R. 1224 does not direct the completion of any specific rule makings within the meaning of 5 U.S.C. 551.

FEDERAL ADVISORY COMMITTEE ACT

The Committee finds that the legislation does not establish or authorize the establishment of an advisory committee within the definition of 5 U.S.C. App., Section 5(b).

UNFUNDED MANDATE STATEMENT

Section 423 of the Congressional Budget and Impoundment Control Act (as amended by Section 101(a)(2) of the Unfunded Mandates Reform Act, P.L. 104–4) requires a statement as to whether the provisions of the reported include unfunded mandates. In com-

pliance with this requirement the Committee has received a letter from the Congressional Budget Office included herein.

EARMARK IDENTIFICATION

H.R. 1224 does not include any congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9 of rule XXI.

COMMITTEE ESTIMATE

Clause 3(d)(2) of rule XIII of the Rules of the House of Representatives requires an estimate and a comparison by the Committee of the costs that would be incurred in carrying out H.R. 1224. However, clause 3(d)(3)(B) of that rule provides that this requirement does not apply when the Committee has included in its report a timely submitted cost estimate of the bill prepared by the Director of the Congressional Budget Office under section 402 of the Congressional Budget Act.

BUDGET AUTHORITY AND CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

With respect to the requirements of clause 3(c)(2) of rule XIII of the Rules of the House of Representatives and section 308(a) of the Congressional Budget Act of 1974 and with respect to requirements of clause (3)(c)(3) of rule XIII of the Rules of the House of Representatives and section 402 of the Congressional Budget Act of 1974, the Committee has received the following cost estimate for H.R. 1224 from the Director of Congressional Budget Office:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, May 2, 2017.

Hon. LAMAR SMITH,
Chairman, Committee on Science, Space, and Technology, House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 1224, the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017.

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

Sincerely,

KEITH HALL,
Director.

Enclosure.

H.R. 1224—NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017

Summary: H.R. 1224 would direct the National Institute of Standards and Technology (NIST) to perform several new duties to promote and audit the compliance of federal agencies with federal guidelines and requirements for managing cybersecurity and other information risks. Based on an analysis of information from NIST and several of the affected agencies, CBO estimates that imple-

menting the bill would cost $48 million over the 2018–2022 period, assuming appropriation of the necessary amounts.

Enacting H.R. 1224 would not affect direct spending or revenues; therefore, pay-as-you-go procedures do not apply. CBO estimates that enacting H.R. 1224 would not increase net direct spending or on-budget deficits in any of the four consecutive 10-year periods beginning in 2028.

H.R. 1224 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would not affect the budgets of state, local, or tribal governments.

Estimated cost to the Federal Government: The estimated budgetary effect of H.R. 1224 is shown in the following table. The costs of this legislation fall primarily within budget function 370 (commerce and housing credit).

	By fiscal year, in millions of dollars—						
	2017	2018	2019	2020	2021	2022	2017–2022
INCREASES IN SPENDING SUBJECT TO APPROPRIATION							
Estimated Authorization Level	0	13	9	9	10	10	51
Estimated Outlays	0	10	10	9	9	10	48

Basis of estimate: For this estimate, CBO assumes that the bill will be enacted late in fiscal year 2017, that the necessary amounts will be appropriated near the start of each year, and that spending will follow historical patterns for the affected agencies.

H.R. 1224 would require NIST to provide all federal agencies guidance on how they can incorporate an existing framework for cybersecurity best practices into their risk management efforts. NIST would be required to identify areas of conflict and gaps between those best practices and current agency requirements, develop a template for agencies to use the framework, recommend other actions agencies should take to comply with federal cybersecurity requirements, and update such guidance as necessary. Based on an analysis of information from NIST, CBO estimates that implementing those provisions would require approximately 20 new staff over nine months and two additional staff throughout the 2018–2022 period to provide agencies with templates and support to incorporate the framework into their cybersecurity efforts. CBO estimates those staff would cost about $3 million over the 2018–2022 period.

H.R. 1224 also would direct NIST to establish and chair a federal working group composed of representatives from several agencies to develop metrics to assess the effectiveness of federal cybersecurity requirements, determine best practices in this area, and compile information on federal agency compliance with such requirements. The Office of Science and Technology Policy and the Office of Management and Budget would be required to issue an annual report on agencies' use and on the effectiveness of federal guidance and requirements. Based on an analysis of information from NIST, CBO estimates that implementing those provisions would cost $5 million over the 2018–2022 period for NIST and federal agencies to participate in the working group and to issue annual reports.

Finally, H.R. 1224 would require NIST to assess the cybersecurity preparedness of federal agencies and, at least biennially, to

audit each agency to determine whether they are complying with best practices according to the metrics developed by the federal working group. NIST would conduct individual audits of agencies whose information security risk is at a high level on an annual basis and all other agencies on a biennial basis. Based on an analysis of information from NIST and the Department of Commerce, CBO estimates that implementing this provision would cost $40 million over the 2018–2022 period and would require about 45 new staff to complete an initial security risk assessment of federal agencies and to conduct the cybersecurity audits of agencies, and for agencies to participate in the audits.

Pay-As-You-Go considerations: None.

Increase in long-term direct spending and deficits: CBO estimates that enacting H.R. 1224 would not increase net direct spending or on-budget deficits in any of the four consecutive 10-year periods beginning in 2028.

Intergovernmental and private-sector impact: H.R. 1224 contains no intergovernmental or private-sector mandates as defined in UMRA and would not affect the budgets of state, local, or tribal governments.

Estimate prepared by: Federal costs: Stephen Rabent; Impact on state, local, and tribal governments: Paige Piper/Bach; Impact on the private sector: John Sperl.

Estimate approved by: H. Samuel Papenfuss, Deputy Assistant Director for Budget Analysis.

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):

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY ACT

* * * * * * *

SEC. 20. (a) The Institute shall—

(1) have the mission of developing standards, guidelines, and associated methods and techniques for information systems*, emphasizing the principle that expanding cybersecurity threats require engineering security from the beginning of an information system's life cycle, building more trustworthy and secure components and systems from the start, and applying well-defined security design principles throughout*;

(2) develop standards and guidelines, including minimum requirements, for information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency, other than national security systems (as defined in section 3552(b)(5) of title 44, United States Code);

(3) develop standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems; and

(4) carry out the responsibilities described in paragraph (3) through the Computer Security Division.

(b) The standards and guidelines required by subsection (a) shall include, at a minimum—

(1)(A) standards to be used by all agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels;

(B) guidelines recommending the types of information and information systems to be included in each such category; and

(C) minimum information security requirements for information and information systems in each such category;

(2) a definition of and guidelines concerning detection and handling of information security incidents; and

(3) guidelines developed in coordination with the National Security Agency for identifying an information system as a national security system consistent with applicable requirements for national security systems, issued in accordance with law and as directed by the President.

(c) In developing standards and guidelines required by subsections (a) and (b), the Institute shall—

(1) consult with other agencies and offices (including, but not limited to, the Director of the Office of Management and Budget, the Departments of Defense and Energy, the National Security Agency, the General Accounting Office, and the Secretary of Homeland Security) to assure—

(A) use of appropriate information security policies, procedures, and techniques, in order to improve information security and avoid unnecessary and costly duplication of effort; and

(B) that such standards and guidelines are complementary with standards and guidelines employed for the protection of national security systems and information contained in such systems;

(2) provide the public with an opportunity to comment on proposed standards and guidelines;

(3) submit to the Director of the Office of Management and Budget for promulgation under section 11331 of title 40, United States Code—

(A) standards, as required under subsection (b)(1)(A), no later than 12 months after the date of the enactment of this section; and

(B) minimum information security requirements for each category, as required under subsection (b)(1)(C), no later than 36 months after the date of the enactment of this section;

(4) issue guidelines as required under subsection (b)(1)(B), no later than 18 months after the date of the enactment of this Act;

(5) ensure that such standards and guidelines do not require specific technological solutions or products, including any specific hardware or software security solutions;

(6) ensure that such standards and guidelines provide for sufficient flexibility to permit alternative solutions to provide

equivalent levels of protection for identified information security risks; and

(7) use flexible, performance-based standards and guidelines that, to the greatest extent possible, permit the use of off-the-shelf commercially developed information security products.

(d) The Institute shall—

(1) submit standards developed pursuant to subsection (a), along with recommendations as to the extent to which these should be made compulsory and binding, to the Director of the Office of Management and Budget for promulgation under section 11331 of title 40, United States Code;

(2) provide assistance to agencies regarding—

(A) compliance with the standards and guidelines developed under subsection (a);

(B) detecting and handling information security incidents; and

(C) information security policies, procedures, and practices;

(3) conduct research and analysis—

(A) to determine the nature and extent of information security vulnerabilities and techniques for providing cost-effective information security;

(B) to review and determine prevalent information security challenges and deficiencies identified by agencies or the Institute, including any challenges or deficiencies described in any of the annual reports under section 3553 or 3554 of title 44, United States Code, and in any of the reports and the independent evaluations under section 3555 of that title, that may undermine the effectiveness of agency information security programs and practices; and

(C) to evaluate the effectiveness and sufficiency of, and challenges to, Federal agencies' implementation of standards and guidelines developed under this section and policies and standards promulgated under section 11331 of title 40, United States Code;

(4) develop and periodically revise performance indicators and measures for agency information security policies and practices;

(5) evaluate private sector information security policies and practices and commercially available information technologies to assess potential application by agencies to strengthen information security;

(6) evaluate security policies and practices developed for national security systems to assess potential application by agencies to strengthen information security;

(7) periodically assess the effectiveness of standards and guidelines developed under this section and undertake revisions as appropriate;

(8) solicit and consider the recommendations of the Information Security and Privacy Advisory Board, established by section 21, regarding standards and guidelines developed under subsection (a) and submit such recommendations to the Director of the Office of Management and Budget with such standards submitted to the Director; and

(9) prepare an annual public report on activities undertaken in the previous year, and planned for the coming year, to carry out responsibilities under this section.

(e) INTRAMURAL SECURITY RESEARCH.—As part of the research activities conducted in accordance with subsection (d)(3), the Institute shall, to the extent practicable and appropriate—

(1) conduct a research program to develop a unifying and standardized identity, privilege, and access control management framework for the execution of a wide variety of resource protection policies and that is amenable to implementation within a wide variety of existing and emerging computing environments;

(2) carry out research associated with improving the security of information systems and networks;

(3) carry out research associated with improving the testing, measurement, usability, and assurance of information systems and networks;

(4) carry out research associated with improving security of industrial control systems;

(5) carry out research associated with improving the security and integrity of the information technology supply chain; and

(6) carry out any additional research the Institute determines appropriate.

(f) As used in this section—

(1) the term "agency" has the same meaning as provided in section 3502(1) of title 44, United States Code;

(2) the term "information security" has the same meaning as provided in section 3532(1) of such title;

(3) the term "information system" has the same meaning as provided in section 3502(8) of such title;

(4) the term "information technology" has the same meaning as provided in section 11101 of title 40, United States Code; and

(5) the term "national security system" has the same meaning as provided in section 3532(b)(2) of such title.

SEC. 20A. FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY.

(a) IMPLEMENTATION BY FEDERAL AGENCIES.—The Institute shall promote the implementation by Federal agencies of the Framework for Improving Critical Infrastructure Cybersecurity (in this section and section 20B referred to as the "Framework") by providing to the Office of Management and Budget, the Office of Science and Technology Policy, and all other Federal agencies, not later than 6 months after the date of enactment of the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017, guidance that Federal agencies may use to incorporate the Framework into their information security risk management efforts, including practices related to compliance with chapter 35 of title 44, United States Code, and any other applicable Federal law.

(b) GUIDANCE.—The guidance required under subsection (a) shall—

(1) describe how the Framework aligns with or augments existing agency practices related to compliance with chapter 35 of title 44, United States Code, and any other applicable Federal law;

(2) identify any areas of conflict or overlap between the Framework and existing cybersecurity requirements, including gap areas where additional policies, standards, guidelines, or programs may be needed to encourage Federal agencies to use the Framework and improve the ability of Federal agencies to manage cybersecurity risk;

(3) include a template for Federal agencies on how to use the Framework, and recommend procedures for streamlining and harmonizing existing and future cybersecurity-related requirements, in support of the goal of using the Framework to supplant Federal agency practices in compliance with chapter 35 of title 44, United States Code;

(4) recommend other procedures for compliance with cybersecurity reporting, oversight, and policy review and creation requirements under such chapter 35 and any other applicable Federal law; and

(5) be updated, as the Institute considers necessary, to reflect what the Institute learns from ongoing research, the audits conducted pursuant to section 20B(c), the information compiled by the Federal working group established pursuant to subsection (c), and the annual reports published pursuant to subsection (d).

(c) FEDERAL WORKING GROUP.—Not later than 3 months after the date of enactment of the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017, the Institute shall establish and chair a working group (in this section referred to as the "Federal working group"), including representatives of the Office of Management and Budget, the Office of Science and Technology Policy, and other appropriate Federal agencies, which shall—

(1) not later than 6 months after the date of enactment of the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017, develop outcome-based and quantifiable metrics to help Federal agencies in their analysis and assessment of the effectiveness of the Framework in protecting their information and information systems;

(2) update such metrics as the Federal working group considers necessary;

(3) compile information from Federal agencies on their use of the Framework and the results of the analysis and assessment described in paragraph (1); and

(4) assist the Office of Management and Budget and the Office of Science and Technology Policy in publishing the annual report required under subsection (d).

(d) REPORT.—The Office of Management and Budget and the Office of Science and Technology Policy shall develop and make publicly available an annual report on agency adoption rates and the effectiveness of the Framework. In preparing such report, the Offices shall use the information compiled by the Federal working group pursuant to subsection (c)(3).

SEC. 20B. CYBERSECURITY AUDITS.

(a) INITIAL ASSESSMENT.—

(1) REQUIREMENT.—Not later than 6 months after the date of enactment of the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017, the Institute shall complete an initial assessment of the cybersecurity preparedness of the agencies de-

scribed in paragraph (2). Such assessment shall be based on information security standards developed under section 20, and may also be informed by work done or reports published by other Federal agencies or officials.

(2) AGENCIES.—The agencies referred to in paragraph (1) are the agencies referred to in section 901(b) of title 31, United States Code, and any other agency that has reported a major incident (as defined in the Office of Management and Budget Memorandum—16—03, published on October 30, 2015, or any successor document).

(3) NATIONAL SECURITY SYSTEMS.—The requirement under paragraph (1) shall not apply to national security systems (as defined in section 3552(b) of title 44, United States Code).

(b) AUDIT PLAN.—Not later than 6 months after the date of enactment of this Act, the Institute shall prepare a needs-based plan for carrying out the audits of agencies as required under subsection (c). Such plan shall include a description of staffing plans, workforce capabilities, methods for conducting such audits, coordination with agencies to support such audits, expected timeframes for the completion of audits, and other information the Institute considers relevant. The plan shall be transmitted by the Institute to the congressional entities described in subsection (c)(4)(F).

(c) AUDITS.—

(1) REQUIREMENT.—Not later than 6 months after the date of enactment of the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017, the Institute shall initiate an individual cybersecurity audit of each agency described in subsection (a)(2), to assess the extent to which the agency is meeting the information security standards developed under section 20.

(2) RELATION TO FRAMEWORK.—Audits conducted under this subsection shall—

(A) to the extent applicable and available, be informed by the report on agency adoption rates and the effectiveness of the Framework described in section 20A(d); and

(B) if the agency is required by law or executive order to adopt the Framework, be based on the guidance described in section 20A(b) and metrics developed under section 20A(c)(1).

(3) SCHEDULE.—The Institute shall establish a schedule for completion of audits under this subsection to ensure that—

(A) audits of agencies whose information security risk is high, based on the assessment conducted under subsection (a), are completed not later than 1 year after the date of enactment of the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017, and are audited annually thereafter; and

(B) audits of all other agencies described in subsection (a)(2) are completed not later than 2 years after the date of enactment of the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017, and are audited biennially thereafter.

(4) REPORT.—A report of each audit conducted under this subsection shall be transmitted by the Institute to—

(A) the Office of Management and Budget;

(B) the Office of Science and Technology Policy;

(C) the Government Accountability Office;

(D) the agency being audited;

(E) the Inspector General of such agency, if there is one; and

(F) Congress, including the Committee on Science, Space, and Technology of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate.

* * * * * * *

MINORITY VIEWS

Cybersecurity is a critically important topic, and one that should attract bipartisan support. Unfortunately, H.R. 1224, the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017 is so ill conceived that I cannot support it in its current form.

The Research & Technology Subcommittee held an excellent hearing on cybersecurity two weeks prior to the Committee's mark-up of H.R. 1224, during which we heard many good recommendations from widely respected experts. Some of those recommendations fell within our Committee's jurisdiction, others did not.

I do remember the panel unanimously praising NIST's role in cybersecurity. I also remember discussion about developing metrics for the adoption of NIST's Cybersecurity Framework. Witnesses also discussed requiring Federal agencies to incorporate the Framework into their information security programs.

I can see where Mr. Abraham has attempted to incorporate some aspects of those recommendations into his legislation. However, I specifically recall GAO's recommendation that the Department of Homeland Security, and *not* NIST, carry out surveys and assessments of the adoption and effectiveness of the Cybersecurity Framework.

NIST itself has steadfastly maintained that they are the wrong agency to do it, and not just because of limited resources.

In addition, I do not remember a single witness, or a single expert recommendation suggesting that OSTP should be given any role in evaluation or oversight of cybersecurity in the private sector or the Federal government. Perhaps if we substituted OMB or DHS for OSTP everywhere in this bill, it might make more sense. The Majority has inserted an entirely new agency into a policy matter in which they have no expertise and no business being a part of. In doing so, the bill also duplicates authorities and responsibilities clearly assigned to OMB and DHS in current law.

Finally, and speaking to what may be the strangest part of this bill, I do not remember any expert ever recommending that NIST be given the responsibility to conduct annual cybersecurity audits of other agencies. NIST is not an auditing agency.

They have no such history, expertise, or capacity. They are a standards and technology agency. In addition, a single FISMA audit costs between a few hundred thousand to a couple of million dollars, depending on the size and mission of the agency. Nowhere in this bill do we provide NIST with the tens of millions of dollars of additional funding required to become the cybersecurity auditing agency of the Federal government. This is a massive unfunded mandate levied on an agency which is already over tasked. Moreover, current law already assigns this very responsibility to agency inspectors general. And no expert I know of has questioned the quality or integrity of the IGs' work. In fact, IGs know and under-

stand their own agencies' business operations and information systems infrastructure better than NIST ever will. In short, I remain thoroughly baffled by the inclusion of this proposal in H.R. 1224.

H.R. 1224 has a number of controversial new elements which were clearly not vetted with the cybersecurity community or the Administration prior to the Committee's markup. In its current form, H.R. 1224 is a counterproductive piece of legislation. I cannot support legislation which will undermine the very agency we are tasking with keeping our cyber infrastructure secure.

EDDIE BERNICE JOHNSON.

○