

In conclusion, God bless our troops, and we will never forget September the 11th in the global war on terrorism.

COMMUNICATION FROM THE CLERK OF THE HOUSE

The SPEAKER pro tempore laid before the House the following communication from the Clerk of the House of Representatives:

OFFICE OF THE CLERK,
HOUSE OF REPRESENTATIVES,
Washington, DC, November 13, 2017.

Hon. PAUL D. RYAN,
The Speaker, House of Representatives,
Washington, DC.

DEAR MR. SPEAKER: Pursuant to the permission granted in Clause 2(h) of Rule II of the Rules of the U.S. House of Representatives, the Clerk received the following message from the Secretary of the Senate on November 13, 2017, at 12:38 p.m.:

That the Senate passed S. 324.
That the Senate passed S. 886.
That the Senate passed S. 906.
That the Senate passed S. 1153.
That the Senate passed S. 1266.
With best wishes, I am

Sincerely,

KAREN L. HAAS.

RECESS

The SPEAKER pro tempore. Pursuant to clause 12(a) of rule I, the Chair declares the House in recess until approximately 4 p.m. today.

Accordingly (at 2 o'clock and 4 minutes p.m.), the House stood in recess.

□ 1601

AFTER RECESS

The recess having expired, the House was called to order by the Speaker pro tempore (Mr. BUCSHON) at 4 o'clock and 1 minute p.m.

ANNOUNCEMENT BY THE SPEAKER PRO TEMPORE

The SPEAKER pro tempore. Pursuant to clause 8 of rule XX, the Chair will postpone further proceedings today on motions to suspend the rules on which a recorded vote or the yeas and nays are ordered, or votes objected to under clause 6 of rule XX.

The House will resume proceedings on postponed questions at a later time.

MARKET DATA PROTECTION ACT OF 2017

Mr. HUIZENGA. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 3973) to amend the Securities Exchange Act of 1934 to require certain entities to develop internal risk control mechanisms to safeguard and govern the storage of market data.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 3973

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Market Data Protection Act of 2017".

SEC. 2. INTERNAL RISK CONTROLS.

The Securities Exchange Act of 1934 (15 U.S.C. 78a et seq.) is amended—

(1) by inserting after section 4E the following:

"SEC. 4F. INTERNAL RISK CONTROLS.

"(a) IN GENERAL.—Each of the following entities, in consultation with the Chief Economist, shall develop comprehensive internal risk control mechanisms to safeguard and govern the storage of all market data by such entity, all market data sharing agreements of such entity, and all academic research performed at such entity using market data:

"(1) The Commission.

"(2) Each national securities association registered pursuant to section 15A.

"(3) The operator of the consolidated audit trail created by a national market system plan approved pursuant to section 242.613 of title 17, Code of Federal Regulations (or any successor regulation).

"(b) CONSOLIDATED AUDIT TRAIL PROHIBITED FROM ACCEPTING MARKET DATA UNTIL MECHANISMS DEVELOPED.—The operator described in paragraph (3) of subsection (a) may not accept market data (or shall cease accepting market data) until the operator has developed the mechanisms required by such subsection. Any requirement for a person to provide market data to the operator shall not apply during any time when the operator is prohibited by this subsection from accepting such data.

"(c) TREATMENT OF PREVIOUSLY DEVELOPED MECHANISMS.—The development of comprehensive internal risk control mechanisms required by subsection (a) may occur, in whole or in part, before the date of the enactment of this section, if such development and such mechanisms meet the requirements of such subsection (including consultation with the Chief Economist)."; and

(2) in section 3(a)—

(A) by redesignating the second paragraph (80) (relating to funding portals) as paragraph (81); and

(B) by adding at the end the following:

"(82) CHIEF ECONOMIST.—The term 'Chief Economist' means the Director of the Division of Economic and Risk Analysis, or an employee of the Commission with comparable authority, as determined by the Commission.".

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Michigan (Mr. HUIZENGA) and the gentleman from California (Mr. SHERMAN) each will control 20 minutes.

The Chair recognizes the gentleman from Michigan.

GENERAL LEAVE

Mr. HUIZENGA. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days within which to revise and extend their remarks and to include extraneous material on this bill.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Michigan?

There was no objection.

Mr. HUIZENGA. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, cybersecurity is critical to consumers, investors, market participants and, frankly, the very markets themselves. However, in April of 2016, the GAO—the Government Accountability Office—identified weak-

nesses regarding information security protocols at the Securities and Exchange Commission, and noted that the SEC's failure to implement an agency-wide data security program had occurred.

Once confirmed in May of this year, SEC Chairman Jay Clayton initiated an assessment of the SEC's internal cybersecurity risk profile and their approach to cybersecurity from a regulatory and oversight perspective. The SEC's internal assessment found that the agency had inadequate controls and that there were serious cyber and data risks.

Unfortunately, in September of this year, Chairman Clayton issued a statement on cybersecurity in which he revealed that a cyber breach "previously detected in 2016 may have provided illicit gain through trading."

Specifically, a software vulnerability existed in the test filing component of the SEC's Electronic Data Gathering, Analysis, and Retrieval—which resulted in access to nonpublic information. While this breach provided hackers access to highly sensitive material, at the time, the SEC believed "the intrusion did not result in unauthorized access to personally identifiable information"—or PII, as we commonly refer to it—therefore, "jeopardize the operations of the SEC, or result in a systemic risk." And that was a quote from the SEC's report.

However, unfortunately, in a follow-up disclosure shortly after that, Chairman Clayton revealed that personally identifiable information, including names, birth dates, Social Security numbers, were actually compromised for two individuals in that particular breach.

The GAO report and the EDGAR data breach underscore what is now even of greater concern, the sufficiency of risk control mechanisms for the SEC-approved consolidated audit trail, or also known as the CAT system. The CAT will be the most comprehensive repository of market data we have seen, and it will collect and identify every order, cancellation, and trade execution for all exchange-listed equities and options across all U.S. markets. It will also collect personally identifiable information beginning 1 year after it begins accepting market data.

Thesys Technologies, which was selected to be the plan processor for the CAT, is scheduled to begin accepting data from self-regulatory organizations who must provide data to CAT on Wednesday, November 15, just merely days from today.

Many of my colleagues, as well as market participants, have voiced concerns about the cost of building and implementing such a system and the amount of PII that will be required to be collected by the CAT.

Last Congress, several Members wrote to former SEC Chair Mary Jo White expressing serious concerns

about the security of such sensitive information held within that CAT system, as well as those who will have access to such information.

As I mentioned, the deadline for the SROs to begin reporting to this CAT system is just 2 days away. It is paramount that the SEC has adequate data security controls in place before that implementation.

Previously, in committee, I had put it this way: That is a repository of the information of gold. Gold is the equivalent of information today. What they are doing is they are putting more gold into that data vault, and we don't have the security to support it.

So while the CAT may be a helpful resource for the SEC, and even the self-regulatory agencies or organizations—SROs—once fully implemented, insufficient data security controls will undermine confidence in our markets and may very well result in the CAT being counterproductive.

Thus, I joined with Financial Services Committee Chairman HENSARLING in writing Chairman Clayton to “encourage the SEC to delay implementation of the CAT system until the SEC can implement information security safeguards and internal controls to ensure the security of confidential and sensitive data.”

No assurances for a delay in implementing the CAT have been provided, and even if they have, it is appropriate for Congress to set baseline standards to ensure that controls are in place. In other words, Mr. Speaker, we are trying to do our job.

H.R. 3973, the Market Data Protection Act, introduced by Representatives DAVIDSON and SHERMAN, is necessary to ensure that the SEC is properly securing critical data that supports our financial markets as well as the personal information of millions of customers with broker-dealer accounts.

Specifically, the bipartisan legislation would mandate that the SEC, FINRA, and the operator of the consolidated audit trail, in consultation with the SEC's chief economist, develop comprehensive internal risk control mechanisms to safeguard and govern the storage of market data, all market data-sharing agreements, and all academic research using that market data.

The bill also halts market data reporting to the consolidated audit trail until the operator of the CAT system develops such internal risk control mechanisms that they are deemed satisfactory.

The EDGAR security breach and the recent massive Equifax data breach—and I might add, Mr. Speaker, we just saw a report of an NSA breach that had just happened, our largest database—well, this would become the second largest database in the country.

Those breaches—in which the sensitive information of nearly 150 million Americans have been compromised, in the Equifax breach—only underscore the importance of proactively ensuring

that any highly sensitive data being collected by the Securities and Exchange Commission or at the SEC's discretion, subject to their oversight, is protected with appropriate safeguards. We owe that to the American people.

The importance of cybersecurity at the SEC cannot be overstated. The SEC's ability to safeguard nonpublic financial information and other highly sensitive data instills confidence in the markets.

SEC Commissioner Michael Piowar recently commented regarding CAT that “deadlines are important, but the SEC has one chance to get this right. We have to make sure that we have everything locked down. We can get it done, or we can get it done right. We need to get it done right.”

I couldn't agree more with Commissioner Piowar. That is why this legislation is so urgently needed. I commend the bipartisan work of Representatives DAVIDSON and SHERMAN, and I urge my colleagues to vote in favor of this very important bill.

Mr. Speaker, I reserve the balance of my time.

Mr. SHERMAN. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I want to commend the sponsor of this legislation, the gentleman from Ohio (Mr. DAVIDSON). It was a pleasure working with him, and I am pleased that he and I introduced this legislation.

This legislation deals with a broader issue of cybersecurity. From Equifax to Moscow, worldwide, people are concerned with cybersecurity. One particular part of cybersecurity that is important is the SEC's accumulation of very sensitive data, whether it be about individuals and their trading, or about the overall market.

In September, the SEC disclosed that hackers had breached the SEC EDGAR database, which is the home to millions of public and nonpublic filings, and that that breach had occurred in 2016. The breach, which was not discovered until August of this year, may have led to some illicit trading activities.

This bill requires the SEC to develop and implement cybersecurity risk controls to ensure that market data is protected. This will help protect our markets from harmful disruptions and manipulative trading.

In addition, this bill requires that FINRA—the Financial Industry Regulatory Authority—and the operator of the new consolidated audit trail develop and implement risk controls to protect the data they store. The new consolidated audit trail system will not accept data until they have the cybersecurity risk controls necessary to protect it.

Once the CAT, or consolidated audit trail, is operational, it will serve an important purpose in assisting the SEC in identifying issues that deserve investigation. But it will also store a large amount of data, and it is impor-

tant that this data be secure. We must ensure that there are proper controls in place.

Now, this bill passed our committee by a vote of 59-1 in its present form. There was an effort after the bill passed committee to try to broaden the bill, and it may very well be that other related issues need to be dealt with by this House. But I think we made the right decision in bringing to the floor today the bill that passed our committee 59-1.

We should then have hearings and perhaps work on additional legislation that will add to our ability to provide for cybersecurity in this area. I look forward to working with the chairman of the subcommittee, and Mr. DAVIDSON, and so many others, on additional legislation designed to ensure our cybersecurity is as good as it can be, and to make sure that we are not putting information into systems unless we are sure that everything has been done so the systems can protect that information.

Mr. Speaker, I call upon all of our colleagues to support this legislation that had 59-1 support in our committee, and I reserve the balance of my time.

Mr. HUIZENGA. Mr. Speaker, I yield such time as he may consume to the gentleman from Ohio (Mr. DAVIDSON), the sponsor of this legislation and a member of the Financial Services Committee.

Mr. DAVIDSON. Mr. Speaker, I appreciate the opportunity to work with Mr. SHERMAN and the rest of the committee on this bill. It is indeed impressive that it was 59-1 in our committee in its present form. It does do some really good things, and I think the message that it really sends is that it is important for our government agency to lead by example.

The SEC holds people that they oversee accountable for maintaining cybersecurity and protecting personally identifiable information.

What we know: on September 20, Chairman Clayton highlighted that they had had a breach of the EDGAR system. This follows on an April 2016 report by the GAO that highlighted some concerns with their cybersecurity program with SEC. The concerning thing is that when Chairman Clayton took over the SEC, he found this so much time afterwards. It wasn't part of his in-briefing. So there is a real concern that there could be some systemic cybersecurity risks there.

I think it is great that our committee came together to provide SEC a mandate to get their own house in order in quick fashion, and to do that with not just their existing products, but with products that are on the cusp of launching: notably, the consolidated audit trail.

□ 1615

The consolidated audit trail became the subject of some additional concerns because it is so close to launching.

What we are trusting here is that Chairman Clayton does the right thing—takes the message from this vote that we are about to take, and then begins to work with our committee to get this cybersecurity risk under control to provide the assurances that the American people want and that the markets need in order to trust that no more data is collected and made vulnerable than is necessary to accomplish the mission, but that whatever data is made available is secure.

Mr. Speaker, I urge all of our colleagues to support the passage of this bill.

Mr. SHERMAN. Mr. Speaker, I urge an “aye” vote. Since I have no speakers seeking time on my side, I yield back the balance of my time.

Mr. HUIZENGA. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, as I had said before, when information is the equivalent of modern-day gold, we need to make sure that whatever vaults that information, that gold, is going into are properly protected—properly protected for consumers and their personally identifiable information. We have an obligation, as the government, to make sure that their information is protected as best as possible, and doubly so when it is going into government-run systems. That is the reason why H.R. 3973 is so imperative that it be passed.

Mr. Speaker, I again commend my friend from Ohio (Mr. DAVIDSON) and my friend from California (Mr. SHERMAN) on their bipartisan work on that.

Mr. Speaker, I urge passage, and I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Michigan (Mr. HUIZENGA) that the House suspend the rules and pass the bill, H.R. 3973.

The question was taken; and (two-thirds being in the affirmative) the rules were suspended and the bill was passed.

A motion to reconsider was laid on the table.

CONNECTED GOVERNMENT ACT

Mr. JODY B. HICE of Georgia. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 2331) to require a new or updated Federal website that is intended for use by the public to be mobile friendly, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 2331

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the “Connected Government Act”.

SEC. 2. FEDERAL WEBSITES REQUIRED TO BE MOBILE FRIENDLY.

(a) AMENDMENT.—Subchapter II of chapter 35 of title 44, United States Code, is amended by adding at the end the following new section:

“§ 3559. Federal websites required to be mobile friendly.

“(a) IN GENERAL.—If, on or after the date that is 180 days after the date of the enactment of this section, an agency creates a website that is intended for use by the public or conducts a redesign of an existing legacy website that is intended for use by the public, the agency shall ensure to the greatest extent practicable that the website is mobile friendly.

“(b) DEFINITIONS.—In this section:

“(1) AGENCY.—The term ‘agency’ has the meaning given that term in section 551 of title 5.

“(2) MOBILE FRIENDLY.—The term ‘mobile friendly’ means, with respect to a website, that the website is configured in such a way that the website may be navigated, viewed, and accessed on a smartphone, tablet computer, or similar mobile device.”.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of sections at the beginning of chapter 35 of title 44, United States Code, is amended by adding after the item related to section 3558 the following new item:

“3559. Federal websites required to be mobile friendly”.

(c) REPORT BY OMB AND GSA REQUIRED.—Not later than 18 months after the date of the enactment of this Act, the Director of the Office of Management and Budget, in consultation with the Administrator of General Services, shall make publicly available and submit to Congress a report that—

(1) describes the implementation of the requirement described under section 3559 of title 44, United States Code, as added by subsection (a); and

(2) assesses the compliance of each agency with such requirement.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Georgia (Mr. JODY B. HICE) and the gentlewoman from Illinois (Ms. KELLY) each will control 20 minutes.

The Chair recognizes the gentleman from Georgia.

GENERAL LEAVE

Mr. JODY B. HICE of Georgia. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days within which to revise and extend their remarks and include extraneous material on the bill under consideration.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Georgia?

There was no objection.

Mr. JODY B. HICE of Georgia. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I rise today in support of H.R. 2331, introduced by the gentlewoman from Illinois (Ms. KELLY). The bill requires all Federal agencies to ensure any Federal Government website intended for use by the public is mobile friendly. Services offered by the Federal Government should be effective but also accessible to the public. Agency websites are one of the most important tools for taxpayers to observe services and information from the government.

The U.S. Government runs more than 6,000 websites on over 400 domains. One recent study estimated that approximately 40 percent of government websites either are not accessible or

are difficult to access on a phone, yet nearly 80 percent of Americans own a smartphone, and at least 1 in 10 American adults rely exclusively on a smartphone for access to the internet, according to a Pew survey. The data clearly points to the utility of making all government websites mobile friendly.

Another study found that more people accessed the internet on their mobile devices than a desktop computer for the first time last year. It is clear that Federal agencies must emphasize mobile accessibility to effectively serve the American people. The Connected Government Act will require agencies to do just that.

This bill requires Federal agencies to ensure their websites are mobile friendly during the course of creating new websites or updating existing ones. A mobile-friendly government is a necessary step in the modernization of the government’s IT infrastructure.

Mr. Speaker, I applaud my colleague, the gentlewoman from Illinois, for her work in sponsoring this bill. I am proud also to support this bipartisan legislation, and I urge my colleagues to do the same.

Mr. Speaker, I reserve the balance of my time.

Ms. KELLY of Illinois. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I include in the RECORD a blog post regarding this bill written by Congressman PALLONE and myself.

[From the Energy & Commerce Democrats, Sep. 13, 2017]

IT’S TIME TO GIVE THE GOVERNMENT AN UPGRADE FOR THE MOBILE WORLD

(By Frank Pallone, Jr. and Robin Kelly)

In the wake of the natural disasters devastating so much of the country, millions of Americans are turning to federal agencies for help—but the government’s websites don’t always make it easy. We’ve introduced legislation in the House that would change that, and it’s moving forward at a time when it can help a lot of Americans who are suffering.

For people who were forced from their homes or are without power because of hurricanes, storms or wildfires, their only connection to necessities of survival—food, water, fuel, and shelter—is through their mobile phones. It’s the device they could take with them when they had to flee their homes. But while private websites and charities have developed new mobile websites and apps to help those who are still struggling, many of the essential government websites on which people depend are essentially unusable on a phone.

During any natural disaster, we expect the government to be at its best. But for people whose homes have been flooded, burned out, or leveled, trying to navigate government websites on their phones likely feels like a waste of time. For instance, if you need to start looking for a loan to rebuild your home, good luck trying to use your phone to navigate the website for the Department of Housing and Urban Development. If you need to reach state or local authorities, the problems get worse. And asking people to hunt down a working desktop computer right now is just unreasonable.

Although these natural disasters are making this problem more acute, the need for a