POVERTY

(Mr. PITTS asked and was given permission to address the House for 1 minute and to revise and extend his remarks.)

Mr. PITTS. Mr. Speaker, it has been more than 50 years since President Johnson declared war on poverty. I don't doubt that President Johnson had good intentions, but intentions don't win wars, and poverty is a stubborn opponent. Fifteen percent of Americans still live below the poverty line, after trillions spent by the government.

In December, I brought together community leaders and national experts to discuss how we can reinvigorate the city of Reading and other cities in the 16th District of Pennsylvania. From this conference, we are moving forward to get institutions to work together strategically and think differently about attacking the problem.

Government at every level and communities leaders need to cooperate and make sure there are opportunities to start new businesses and attract more development.

Perhaps most importantly, we need smart strategies to help kids get a good education. This has to include building strong families, since statistics show that children raised by only one parent are far more susceptible to temptations of drugs and gangs and other problems.

It is time we rethought our strategy and rededicate ourselves to try helping needy Americans by removing barriers for wealth creation.

□ 0915

UNEMPLOYMENT INSURANCE EXTENSION

(Mr. VARGAS asked and was given permission to address the House for 1 minute and to revise and extend his remarks.)

Mr. VARGAS. Mr. Speaker, I rise today to urge my colleagues to extend the critical unemployment insurance lifeline to the 1.3 million Americans who have already lost coverage.

Tragically, another 1.9 million Americans are set to lose benefits over the first 6 months of this year if we do not act. In California alone, over 214,000 people have already lost their unemployment coverage, including 19,000 people in San Diego County and 3,500 people in Imperial County.

Approximately 326,000 more Californians stand to lose their coverage in the first 6 months of 2014. With unemployment unacceptably high, now is not the time to take money out of the pockets of those who are struggling.

For jobless Americans, unemployment benefits are used to purchase basic lifeline needs like food and shelter and immediate necessities. The time is clicking. Let's do the right thing.

HEALTH EXCHANGE SECURITY AND TRANSPARENCY ACT OF 2014

GENERAL LEAVE

Mr. PITTS. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days to revise and extend their remarks and to include extraneous material on H.R. 3811.

The SPEAKER pro tempore (Mr. COLLINS of Georgia). Is there objection to the request of the gentleman from Pennsylvania?

There was no objection.

Mr. PITTS. Mr. Speaker, pursuant to House Resolution 455, I call up the bill (H.R. 3811) to require notification of individuals of breaches of personally identifiable information through Exchanges under the Patient Protection and Affordable Care Act, and ask for its immediate consideration in the House.

The Clerk read the title of the bill.

The SPEAKER pro tempore. Pursuant to House Resolution 455, the bill is considered read.

The text of the bill is as follows:

H.R. 3811

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 ''Health Exchange Security and Transparency Act of 2014''.

SEC. 2. NOTIFICATION OF INDIVIDUALS OF BREACHES OF PERSONALLY IDENTIFIABLE INFORMATION THROUGH PPACA EXCHANGES.

Not later than two business days after the discovery of a breach of security of any system maintained by an Exchange established under section 1311 or 1321 of the Patient Protection and Affordable Care Act (42 U.S.C. 18031, 18041) which is known to have resulted in personally identifiable information of an individual being stolen or unlawfully accessed, the Secretary of Health and Human Services shall provide notice of such breach to each such individual.

The SPEAKER pro tempore. The gentleman from Pennsylvania (Mr. PITTS) and the gentleman from New Jersey (Mr. PALLONE) each will control 30 minutes.

The Chair recognizes the gentleman from Pennsylvania.

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

Mr. Speaker, in the days leading up to Christmas, hackers stole millions of credit card numbers from the servers of retail giant Target. I imagine that at least a few here in this Chamber may have had their own credit cards replaced to prevent theft.

What if Target had not bothered to tell anyone?

What if they had waited until people noticed fraudulent charges popping up on their statements? The damage would certainly be worse.

It may shock some people to learn that there is no legal requirement that the Department of Health and Human Services notify an individual if his or her personal information is breached or improperly accessed through the Affordable Care Act's exchanges.

While HHS has said that it will notify individuals in such a case, the American people have a right to know that their government is required by law to contact them if their personal information is compromised.

H.R. 3811, the Health Exchange Security and Transparency Act, would simply ensure Americans receive notification from HHS when their personally identifiable information has been compromised through the exchanges. Specifically, the bill requires HHS to notify individuals no later than two business days after discovery of a breach of an exchange system.

Since the disastrous rollout of the healthcare.gov Web site, congressional oversight has uncovered that end-to-end security testing of healthcare.gov did not occur before the October 1 launch, and that high-ranking administration officials were told of the security risks before the Web site went live.

Teresa Fryer, the chief information security officer for the agency running the exchange system, even stated in a draft memo that the Federal exchange ''does not reasonably meet security requirements'' and ''there is also no confidence that personal identifiable information will be protected.''

A recent article in Information Week discussed a report released by Experian entitled ''2014 Data Breach Industry Forecast,'' which stated that ''the health care industry, by far, will be the most susceptible to publicly disclosed and widely scrutinized data breaches in 2014.''

According to Information Week, the author of the study said he is basing this prediction at least partly on reports of security risks posted by the healthcare.gov Web site and the health insurance exchanges established by various States. The Web infrastructure to support health insurance reform was ''put together too quickly and haphazardly.''

The most glaring problem for these sites has been their inability to keep up with consumer demand. The organizational infrastructure behind the implementation of ObamaCare is also complex, meaning that many parties have access to the personal data and could misuse or mishandle it.

So we have volume issues, security issues, multiple data handling points, all generally not good things for protecting protected health information and personal identity information.

Given the lack of security testing and the risk associated with healthcare.gov, and the administration's repeated misrepresentation of the Web site's readiness and functionality, H.R. 3811 is a reasonable step to ensure Federal officials are required to notify individuals in case of a breach.

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

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

First of all, Mr. Speaker, I want to point out that Republicans are using

out-of-context quotes from an administration, or from administration officials, to mislead the public about the security of healthcare.gov, the Web site.

The same official they keep quoting went on to say:

> The added protections that we have put into place are best practices above and beyond what is usually recommended. And no Web site is 100 percent secure. But this effort to scare people from signing up for coverage is simply wrong.

Mr. Speaker, I am afraid the bill before the House today is simply an effort by Republicans to continue to impede the efforts of implementing the Affordable Care Act by instilling misinformation and fear in the American public. It is an egregious bill that would, in my opinion—let me point this out, Mr. Speaker. Yesterday, I was in the Rules Committee, and I pointed out that, to some extent, I was pleased, I guess, that I don't see the Republicans actually coming to the floor today to act on another repeal or outright repeal of the Affordable Care Act. I mean, we are not seeing that. We didn't see it in Rules. And hopefully, I will say to my colleague, the chairman of the Health Subcommittee, that we don't see it again, either in the committee, in Rules, or on the floor.

So maybe there is some progress here, and at least the Republicans are not out there trying to repeal the Affordable Care Act anymore—at least I hope so.

But they are now moving to these other methods of trying to put fear in the public so that they don't sign up or they don't go on the Web site. And the fact of the matter is that these security measures that they are talking about are addressing a reality that is not there.

Do I think that security measures are critical for the Web site?

Yes, absolutely. But let's recap the last few years since the ACA passed. Republicans claim the ACA kills jobs; but since the law has passed, we have added nearly 8 million jobs.

Republicans claim that the ACA causes health costs to increase, but the last 4 years we have seen the slowest health care cost growth in 50 years.

Republicans claim we need to address the deficit; yet they repeal the law at every turn, which increases the deficit by over $1.5 trillion.

Well, now they say that healthcare.gov is going to result in widespread breaches of people's personal information, and that is simply not true. There have been no successful security attacks on healthcare.gov, and no one has maliciously accessed personal information.

No Web site, public or private, is 100 percent secure, but healthcare.gov is subject to strict security standards. It is constantly monitored and tested, and its security and privacy protections go beyond Federal IT standards.

And the Health and Human Services Department has standards in place, just like every other government agency, to notify individuals if their personal information is breached.

So, Mr. Speaker, it is important that I note for everyone that House Democrats have always previously supported legislation to require consumer notification in the event of a breach of government and private sector computer systems. We still do.

By expressing concern for the mockery of this bill, it does not mean that I don't support requiring the administration to notify individuals of breaches of their information, but this not is a serious effort to strengthen privacy laws or to strengthen the health care Web site.

The Republican strategy is to scare people away from going to the Web site and signing up for health care, and I urge Members and the American public, do not be fooled by what they are doing.

It is a good thing that they are not seeking to outright repeal the Affordable Care Act anymore, at least that appears to be the case, based on what happened in Rules the other night. But that doesn't mean that they are not going to continue with these efforts to try to make hay over security and other matters.

And I can't stress enough that every one of the scare tactics they use, whether it is saying that the ACA is going to increase the deficit, which it doesn't, it actually decreases the deficit; or whether they say that it is going to increase health costs, which we know it doesn't, it actually decreases health costs.

This is just another one of those scare tactics. And I just hope that my colleagues, both Democrats and Republicans, are not fooled by this.

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

Mr. PITTS. Mr. Speaker, at this time I am pleased to yield 2 minutes to the gentleman from California (Mr. ISSA), the distinguished chairman of the Oversight and Government Reform Committee.

Mr. ISSA. Mr. Speaker, famously, Franklin Delano Roosevelt said, We have nothing to fear but fear itself. That is not true here and, sadly, the last speaker is entitled to his opinion, but the facts do not bear out his conclusions.

The truth is that actual interviews and depositions taken of the highest-ranking people that helped develop this Web site, both public and private, show there was no end-to-end testing. It did not meet the spirit of any definition of a secure Web site.

In fact, the highest-ranking person, Teresa Fryer, on September 20, was unwilling to recommend this site go active, and said under oath that if it had been within her authority to stop it, she would have.

It is very clear, even from the White House's statements in the last few days, that they claim to have mitigated or have a plan to mitigate significant security risks. The American people need to understand a plan to mitigate means they have not mitigated security risks.

This is the situation we are in, in which no private sector company, including Target, would go live with a system that has known failures and unknown failures because of a failure to do end-to-end.

All we are asking for is, since Secretary Sebelius, under oath, has been wrong on multiple occasions, I have called for her to make clear that she made false statements. The fact is what we need is a law that makes it clear that they should do the right thing, not say they have always done the right thing and they will do the right thing, because in the case of healthcare.gov, they launched a site that was neither functionally ready, nor had it been security tested, and it had known failures that were not mitigated prior to the launch.

Those are the facts, Mr. Speaker, and I ask for support of this bill.

Mr. PALLONE. Mr. Speaker, I yield 3 minutes to the gentlewoman from Colorado (Ms. DEGETTE).

Ms. DEGETTE. Mr. Speaker, some mornings in Congress I wake up and I say, now here is a solution in search of a problem; and this morning is one of those days.

We are hearing about how the Web site is not secure, how there can be security breaches. Ironically, we are hearing about security breaches with a private company, Target, and how terrible it is, and that is why we have to do a bill.

But, in fact, we haven't seen any security breaches with healthcare.gov or the Web sites around the Affordable Care Act. And I want to stress that.

□ 0930

I am the ranking Democrat on the Oversight and Investigations Subcommittee of Energy and Commerce, and we have had a number of hearings, and we have had classified briefings. Here is some information that is not classified information.

There has been not one successful hack into www.healthcare.gov. Let me say that again. Nobody has successfully been able to breach www.healthcare.gov. Furthermore, as we have recently learned in a briefing, www.healthcare.gov, interestingly, has not been targeted any more than any other Federal Web site for hackers.

So why are we doing this bill? I have got to associate myself with Ranking Member PALLONE's comments, that the only reason we could be doing this bill is to try to have a chilling effect against people signing up to get health insurance through the Web sites.

Let me say it again. There have been no successful breaches of www.healthcare.gov.

Now, if we really wanted to do a bill that would strengthen privacy, I would be all for that. I think that consumer privacy is one of the most important

things we can do. But really, when you look at the details of this bill, there is nothing here that furthers consumer notification or consumer privacy.

First of all, there is no exemption or consideration of law enforcement. What if law enforcement found a potential breach and needed to investigate it? What if they needed more than 48 hours to make sure that, in fact, there was a breach before they notified people? Consider the harm that would occur if law enforcement did not have enough time and resources to fully investigate a security breach before it went public. The consequences of hasty and incorrect notification could just make the problem worse.

Secondly, based on how the bill is drafted, if there is a data breach in a State that has chosen to run its own exchange, like my home State of Colorado, HHS seems to bear an unnecessary burden of reporting the breach in the State exchange having nothing to do with the Federal exchange.

Might I remind my colleagues, State exchanges are entirely independent from www.healthcare.gov. HHS does not run them. HHS did not build their Web sites, and HHS did not develop their security protocols. So why should HHS have to get involved in the State-run exchanges?

The SPEAKER pro tempore. The time of the gentlewoman has expired.

Mr. PALLONE. Mr. Speaker, I yield an additional 1 minute to the gentlewoman from Colorado.

Ms. DEGETTE. So security for these State-based exchanges should be the responsibility of the States that are running them.

I could go on and on. There are more problems with this bill than pages in the bill.

So let's get real. Instead of bringing legislation like this to the floor without any committee action, why can't we sit down together in a bipartisan way and improve the way the Affordable Care Act works for our constituents? That is what our constituents want. They want affordable health insurance. They want health care. And they don't want unwarranted scare tactics and attacks. So let's sit down. Let's work together. Let's fix this legislation. And let's get real.

Mr. PITTS. Mr. Speaker, I am pleased, at this time, to yield 2 minutes to the distinguished gentlelady from Tennessee (Mrs. BLACK), who is an expert on this issue.

Mrs. BLACK. Mr. Speaker, I rise today in support of this legislation to provide basic diligence to the Federal ObamaCare exchange.

If someone's personal information has been breached, the Federal Government should be accountable and be required to notify them so that they can protect themselves from either identity theft or cyber threats.

This is common sense, as data breach notification is required on most of the State-run exchanges, and there are laws that require notification by private businesses as well. Yet, when HHS was asked to insert notification provisions into the final rule for ObamaCare, they specifically declined to do so. This is an astonishing failure on the part of the administration though, sadly, characteristic of how they have proceeded at every turn with implementation of this train wreck legislation.

www.healthcare.gov has been described by former Social Security Administrator Michael Astrue as a ''hacker's dream,'' and last month, HHS reported that there had been 32 security incidents since its launch. The Federal exchange potentially puts at risk Americans' names, addresses, phone numbers, dates of birth, email addresses, and even Social Security numbers.

Last month, I introduced similar data breach notification legislation, and I am pleased to join my House colleagues now to pass this important bill.

Mr. Speaker, I can't imagine explaining to my constituents that I voted against this commonsense measure to protect hardworking Americans from identity theft and cyber attacks, and this is why I urge my colleagues to support this bill.

Mr. PALLONE. Mr. Speaker, I yield 3 minutes to the gentleman from Maryland (Mr. CUMMINGS), the ranking member of the House Committee on Oversight and Government Reform.

Mr. CUMMINGS. Mr. Speaker, I thank the distinguished gentleman from New Jersey for yielding.

I would like to make two very, very simple points.

First, the Affordable Care Act is working. Hello. It is working. It went into full effect, if you didn't know, on January 1, and now millions of people—millions—are getting health insurance that they didn't have before.

Imagine what this means to families. Not only are they receiving critical medical care, but they have the security of knowing they will not go bankrupt if they get into an accident or they get sick. That is major.

The law also put in place key protections for consumers. Insurance companies are now prohibited from discriminating against people with cancer, diabetes, or other preexisting conditions. Some young people in my district said, Well, Congressman, I am not worried about preexisting conditions. I told them, You just keep on living. Insurance companies may not charge higher prices for women, and millions of people are now receiving free preventative care.

There are also huge financial benefits. Health insurance companies are sending rebate checks to millions of people. Since the law was passed, we have seen the lowest growth in health care costs in 50 years; and if we repealed the law today, it would increase our deficit by more than $1.5 trillion.

Despite all these positive results, Republicans are still obsessed with killing the law. Since they cannot do it legislatively, they have shifted to a different tactic—scaring people away from the Web site.

So my second point is this. There have been no successful security breaches of www.healthcare.gov. Let me say that again. There have been no successful security breaches of www.healthcare.gov. Nobody's personal information has been maliciously hacked.

All week, Republicans have been trying to make their case for this bill by quoting from a memo drafted by the chief information security officer at CMS about concerns before the Web site was launched, but they omit one critical fact: this official never sent the memo. It was a draft. And she never gave it to anyone, including her own supervisor. How do we know this? Because she was interviewed by the Oversight Committee by both Republican and Democratic staff weeks ago.

The SPEAKER pro tempore. The time of the gentleman has expired.

Mr. PALLONE. I yield the gentleman from Maryland an additional 1 minute.

Mr. CUMMINGS. And she told us this herself.

Her draft memo did not take into account mitigation strategies put in place in the days that followed. Importantly, she also told the committee that she is satisfied with the security testing being conducted. When asked to describe the security measures now in place, she called them, ''best practices above and beyond what is usually recommended.''

These are important facts for the American people to know, but the Republicans disregard them and omit them because they want to undermine their claims.

Many of us would support efforts to strengthen requirements for the entire Federal Government and private sector to notify consumers of breaches, but today's bill does not do that. Today's bill is the latest attempt to attack the Affordable Care Act and deprive millions of Americans of the health care they deserve.

Mr. PITTS. Mr. Speaker, at this time, I am pleased to yield 1 minute to the gentleman from California, KEVIN MCCARTHY, the distinguished whip of the House.

Mr. MCCARTHY of California. Mr. Speaker, I rise today in support of the Health Exchange Security and Transparency Act. The reason why we are passing this important legislation today is that credible and documented fears have been raised that this hastily constructed ObamaCare exchange Web site could jeopardize the security of our most sensitive personal information.

One of the many reasons so many worry about ObamaCare is that it injects government and government bureaucrats into the most personal sphere of our lives, our health care, in new and alarming ways. Nothing could turn a life more upside down quickly than identity theft. It is our duty, as Members of Congress, to do everything

in our power to protect and inform Americans about these potentially devastating events.

I am confident that this concern is one of the law's most negative consequences that both sides of the aisle can come together and agree must be addressed. Absent its full repeal, instilling this type of transparency and accountability into ObamaCare is a worthy first step. I urge my Democratic friends to join with us today.

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

Mr. Speaker, Republicans continue to attack the Web site, www.healthcare.gov, and this attack on the security of the Web site is just the latest in a long line of scare tactics attempting to limit enrollment and coverage under the ACA.

It just bothers me so much because, as you know now, we have about 6 million people who have obtained coverage, 2.1 million receive private insurance through the Web site, and things really are moving now in terms of more and more people signing up and getting coverage.

I just wish that, rather than using scare tactics and trying to talk about security concerns that don't exist, they would focus and work with us at actually trying to sign people up to get people to have health insurance, which is the goal, of course, of the Affordable Care Act.

The bill suggests that there are serious security problems with www.healthcare.gov, but this unique requirement doesn't apply to other government Web sites or to private Web sites. Under the bill, HHS is required to notify individuals within 2 business days if their personally identifiable information is known to be stolen or unlawfully accessed from a marketplace computer system. If this is a good idea, then why is the GOP bill limiting this requirement to only marketplace Web sites? It is just a missed opportunity.

Democrats firmly support strong data security and breach notification legislation. If the Republicans were serious about the security of personally identifiable information on the Web, instead of bringing up this bill, they could have reached out to Democrats and developed a bipartisan bill.

Indeed, when Democrats were in the majority, the Democrat-run House passed bipartisan legislation to provide for consumer notification in the event of a breach, which was introduced in the previous Congress. And the Republicans are still playing political games. If they want to work with us to bring to the floor serious bipartisan data security breach notification legislation, then they should simply do it.

In the Rules Committee the other day, one of the members asked, on the Republican side, if the administration has a position on the bill. And the administration clearly opposes the bill. They put out an SAP which states:

> The Administration believes Americans' personally identifiable information should be protected wherever it resides, and that all Americans deserve to know if that information has been improperly exposed . . . The Federal Government has already put in place an effective and efficient system for securing personally identifiable information in the Health Insurance Marketplaces.

So they oppose the passage of this bill.

I just wish I could convince my colleagues—again, I am happy that this is not an outright repeal and that we are not wasting time on that, but we are still wasting time with this notion of the security breach that hasn't happened when security measures are already in place.

Again, this is being brought up in the first week we are back with no effort to reach out to us in any way to try to deal with this. It has a 2-day notification requirement, which is simply not workable.

I cannot stress enough that we, as Democrats, would like to address this issue, but it is not being addressed. It is just being done as a way of trying to scare the public from signing up on the Web site, which is so unfortunate because people want to sign up. They shouldn't be in fear that, if they sign up, somehow there is going to be a security breach.

I reserve the balance of my time.

□ 0945

Mr. PITTS. Mr. Speaker, at this time, I am pleased to yield 4 minutes to the gentleman from Florida (Mr. BILIRAKIS), a distinguished member of the Health Subcommittee.

Mr. BILIRAKIS. Thank you, Mr. Chairman. I appreciate it very much.

Mr. Speaker, I rise today in support of the Health Exchange Security and Transparency Act. I am pleased to be an original cosponsor of this legislation, and I am glad we are addressing this very important issue on the House floor today.

Each day, I hear from constituents in Florida's 12th Congressional District who are experiencing the negative impacts of ObamaCare. Contrary to the very promises the law was sold on, my constituents have lost their health care coverage, have seen their premiums rise, and were forced to choose new doctors. Now they are faced with concerns regarding their personal information and whether it is compromised—all because the President's signature law was never really ready for prime time.

The Energy and Commerce Committee, which I am a member of, has held numerous hearings into the failed Web site and the lack of testing that occurred to ensure the Web site was properly secured.

In these hearings, we have learned that 30 to 40 percent of the Web site isn't built; end-to-end security testing wasn't performed; and CMS' own chief security information officer recommended against an Authority to Operate because of cybersecurity concerns.

Her memo even stated:

> There is no confidence that personally identifiable information will be protected.

It was the administrator of CMS, not that chief information officer, that signed off on the ATO.

Mr. Speaker, does this sound like a safe and secure Web site? Millions of Americans were forced to sign up for the exchanges in order to avoid individual mandate fines. And now each of these individuals, including myself and many in this Chamber, are potential victims of identity theft.

While privacy in the health care realm is typically protected by HIPAA, it does not apply to HHS or the federally run exchanges. Furthermore, data notification is critical to maintaining security, and individuals should be notified when their personal information could be compromised. Yet, in the final rules HHS published in August, it did not finalize a data breach notification rule. Instead, it stated that it is up to ''CMS to determine whether a risk of harm exists and if individuals need to be notified.''

A government bureaucrat, Mr. Speaker, should not be given the power to determine whether the loss of personally identifiable information constitutes harm. We do not know how many breaches have occurred on healthcare.gov, whether due to the accidental sharing of information or otherwise, because there is currently no public disclosure requirement. The Health Exchange Security and Transparency Act will bring accountability and transparency to the administration and the health care exchanges.

I strongly urge my colleagues in the House to support this bill today, and I urge all, of course, our colleagues in the Senate to swiftly take up this bill so that we may pass it into law.

Mr. PALLONE. Mr. Speaker, I yield such time as he may consume to the gentleman from California (Mr. WAXMAN), ranking member of the Energy and Commerce Committee.

Mr. WAXMAN. The previous speaker in this debate said that we don't know how many times there was a breach of security on the health care Web site. Well, we do know how many breaches of security there were, how many successful attacks there were—zero. There have been no successful breaches of healthcare.gov.

Mr. Speaker, since October 1, more than 6 million Americans have signed up for health insurance—6 million. Four million are enrolled in Medicaid, 2 million in private coverage. Any way you look at it, that is good news.

Now Republicans seem eager to find some bad news. They want to keep talking about Web site problems and stir up phony fears that personal information is not secure on this site. They are looking for the bad news because the facts are against them.

Republicans said the Affordable Care Act would kill jobs. We hear it over and over again—kill jobs. Since the law was passed, we have added nearly 8 million jobs. Republicans said this law

would cause health care costs to skyrocket, but we have had 4 straight years of the slowest health care cost growth in 50 years. Republicans said the ACA would explode the deficit, but repealing the law, which they have tried to do over 40 times on the floor, would increase the deficit by over $1.5 trillion.

So, today, House Republicans are resorting to scare tactics. They are bringing up a poorly thought-out bill based on the false premise that healthcare.gov is not secure. The truth is—I will say it again—there have been no successful security attacks on healthcare.gov.

Now, while no site, public or private, is 100 percent secure, healthcare.gov is subject to strict security standards, it is constantly monitored and tested, and it has procedures in place to notify consumers in the event of a breach. We can't say the same thing for private Web sites. We all heard about Target having their Web site attacked successfully. No one is asking that they make disclosures.

In fact, Mr. Speaker, this is not a serious attempt to address this issue because it doesn't set any standards on private insurance companies. Private insurance companies hold far more private data than the exchanges.

Mr. Speaker, as chairman, I worked on bipartisan legislation to set tough data privacy and security standards on government and private sector computer systems. House Democrats have supported these efforts, but this bill is not serious. Did you know this bill was never even considered in committee? It doesn't allow for any delay in reporting to protect ongoing law enforcement investigations. The bill creates a host of technical and administrative problems.

This is purely a message bill. That is all we do these days. In between recesses, we have message bills on the floor of the House, and we get nothing done. This is purely a message bill, and the message is one that is designed to mislead. I urge a ''no'' vote.

Mr. PITTS. Mr. Speaker, at this time, I am pleased to yield 1 minute to the gentleman from Virginia, ERIC CANTOR, our distinguished majority leader.

Mr. CANTOR. I thank the gentleman from Pennsylvania.

Mr. Speaker, I want to rise in support of the Health Exchange Security and Transparency Act. If I could just take a few seconds to respond to the allegations put forward by the gentleman from California, the ranking member on the Energy and Commerce Committee, I want to just make a point, Mr. Speaker. There is a real difference between users of a retailer's Web site and users of healthcare.gov because those who choose to go on the Web site of a retailer in the private sector do so at their choice.

The people of this country, all of the American people now, if they go to healthcare.gov, they are being forced to go to healthcare.gov, and so for the gentleman to sit here and say, well, we don't require this out of the other industries, banks or anything else, I would beg to differ. There are certainly requirements in law and duties owed by banks to their shareholders, customers and the rest, but I would say to the gentleman, this is a situation where the law at hand is requiring individuals—mandating them—to go to this site.

So contrary to the allegations made by the gentleman, what this bill does is it just requires the administration to provide 48 hours' notice after a breach of health care information or financial data. All it says is the administration has to let victims of identity theft or information theft be notified. That is it. This is a good government bill. Why do we want to wait until there is a data breach?

I would ask the gentleman to look to a quote by CMS' own chief information security officer, Teresa Fryer. She said that the Federal exchange ''does not reasonably meet security requirements.'' That is what the chief cybersecurity officer at the agency says, the exchange ''does not meet security requirements.''

Now, the Experian credit bureau said:

> The health care industry, by far, will be the most susceptible to publicly disclosed and widely scrutinized data breaches of 2014.

If we know this, why wouldn't we take precautions to help people? That is all this bill does. It says if there is a risk of data breach, we should afford people the opportunity to take corrective action immediately. That is it. There is no message in there. This is just trying to help people.

So I would say to the gentleman, if he would just set aside the partisan attacks for once, let's help people. Let's go about the way we should be in putting people first here. We disagree on this law in requiring health care the way government says we should require, yes, but I think we can all agree we want to help people, and we want to make sure that they can keep their information safe. That is all this bill is about.

So I want to thank Chairman FRED UPTON, Chairman JOE PITTS, and the members serving on the committees who have been conducting oversight on the issue for the past year, including the Science Committee, the Homeland Security and the Oversight and Government Reform Committees. Congresswoman DIANE BLACK, certainly the gentleman from Florida, GUS BILIRAKIS, and Representative KERRY BENTIVOLIO have all worked hard on this issue. I commend them for their efforts to just help people for once.

With that, I urge adoption and passage of the bill.

Mr. PALLONE. Mr. Speaker, I yield such time as he may consume to Mr. WAXMAN.

Mr. WAXMAN. Well, thank you for yielding. I am not going to take that much time, but I do want to respond to the comments that were just made on the House floor.

No one is forced to go on this Web site. No one is forced to buy their insurance by going on the Web site. They could go to brokers. Once you sign up for insurance, whether it is public or private, your information is in their Web. It is in their computer system. That is true for private insurance. Does this bill do anything about breaches of private insurance? No.

Now, the majority leader used a quote from someone in the administration, I think, to mislead the public about the security of healthcare.gov, but that same official said at the end of that quote, The added protections that we have put into place are best practices above and beyond what is usually recommended.

No Web site is 100 percent secure, but this effort to scare people from signing up for coverage is wrong. If we do care about breaches in security, it ought to apply to private and public insurance, not just when you sign up, but when they hold your data.

Mr. PITTS. Mr. Speaker, at this time, I am pleased to yield 3 minutes to the gentleman from Michigan (Mr. UPTON), the distinguished chairman of the Energy and Commerce Committee.

Mr. UPTON. Mr. Speaker, I rise in strong support of this legislation, H.R. 3811, the Health Exchange Security and Transparency Act of 2014.

Security and transparency are both critically important to every American, and the public expects and deserves to have them both when it comes to health care.

Sadly, I believe the administration has failed to deliver. This important bill seeks to provide peace of mind to folks in Michigan and across the country who have submitted personal information to a Federal health insurance exchange. Americans have the right to know in the event that their sensitive personal information provided to an exchange is compromised, especially as it is the law's individual mandate that forces them to purchase the government-approved health care coverage. Why wouldn't we want the public to know and be alerted right away?

Just this morning on CNBC's ''Breaking News,'' the CEO of Target apparently is indicating that as many as 70 million Americans—their customers—may have had their private information stolen. Would it have been right for Target just to sit on that information? Or was it appropriate for them to try and put the word out so that at least the consumers would have the right information?

□ 1000

Let me tell you what this bill does. It is a commonsense bill. It is going to require that the administration promptly inform individuals within 2 business days if their personal information has been stolen or unlawfully accessed through an exchange. Through the Energy and Commerce Committee's thoughtful oversight, we have uncovered troubling information regarding

the security of the health insurance exchanges. What this bill does is preventive medicine. Do we want to wait until the horse is out of the barn before we take action? I don't think so.

We found that the administration did not perform a full security control assessment before healthcare.gov opened for business on October 1. We have also learned that just days before healthcare.gov went live, senior officials at HHS expressed serious concerns regarding the protection of personally identifiable information that was entered into their Web site.

These facts, on top of the fact that the administration has repeatedly misrepresented the functionality and the readiness of the health care law, raise significant questions regarding the security of healthcare.gov and the information available in the exchanges.

A few weeks ago, the administration was willing to let millions of Americans lose their health insurance, despite the President's solemn promise that they could keep their health plan if they liked it; and it took the House, acting in a bipartisan legislative manner, for the administration to confess that, yes, they had broken their promise.

Now the administration is saying it opposes this requirement that it notify Americans when personal information is stolen.

The SPEAKER pro tempore. The time of the gentleman has expired.

Mr. PITTS. I yield an additional 30 seconds to the gentleman.

Mr. UPTON. So the self-proclaimed, most-transparent administration in history has come out against transparency. I am sorry Republicans and Democrats may disagree on the merits of the President's health care law, and we do; but I think that we should all agree that Americans deserve to be notified if that personal information is put at risk by the law.

I want to thank Chairman PITTS for putting security and transparency above politics, and I would urge my colleagues in a bipartisan way to support this bill this morning.

Mr. PALLONE. Mr. Speaker, I yield 2 minutes to the gentleman from New York (Mr. CROWLEY), the vice chair of the Democratic Caucus.

Mr. CROWLEY. I thank my friend from New Jersey for yielding me this time.

Mr. Speaker, there are so many truly pressing issues facing our Nation, so it is a shame that we are here once again wasting time on legislation like this. It doesn't even solve the issues the Republicans claim they are trying to address. The truth is, the bill we are considering today is far from a productive answer to anything. It is just yet another scare tactic to discourage people from obtaining health care—that is right. Here is a news flash for you: Republicans want to stop people from attaining health care.

I don't think why we should expect anything else from a party with such little vision. Instead of creating opportunity, they have become the party that shuts things down. They shut down the government. They shut down unemployment insurance for people who are desperately trying to find work. They have tried repeatedly to shut down the Affordable Care Act. As a matter of fact, 47 times—47 times—they have attempted to shut down the Affordable Care Act. Heck, they are even shutting down bridges in New Jersey. The fact is, it seems like their agenda is just about shutting down things that actually work for American families. Republicans can't just slam the door shut again and again on the American people. It is time to end this shutdown mentality once and for all here in Washington and get back to working on issues of concern to the entire Nation.

Mr. PITTS. Mr. Speaker, may I inquire of the time remaining.

The SPEAKER pro tempore. The gentleman from Pennsylvania has 13 minutes remaining, and the gentleman from New Jersey has 6½ minutes remaining.

Mr. PITTS. Mr. Speaker, I yield 2 minutes to the gentlewoman from Tennessee (Mrs. BLACKBURN), the vice chair of the Energy and Commerce Committee.

Mrs. BLACKBURN. Mr. Speaker, when is this administration finally going to start paying attention to the warning signs?

When career staff at OMB warned the administration that Solyndra wasn't ready for prime time, they moved forward anyway and lost hardworking taxpayers a half billion dollars.

When private consultants told the White House and HHS officials last spring that there were problems with healthcare.gov, they moved forward anyway.

When CMS sent a memo just 4 days before healthcare.gov went live and warned about ''inherent security risks''—their terminology—the administration moved forward anyway. So their failed policy of forward is costing us money and is getting people into trouble. This is what we are hearing from an Experian report. America's personal information is at high risk on healthcare.gov. There is a great opportunity for a data breach.

Mr. Speaker, this is something we can stop. The bill today does that. It is simple. It addresses the problem. What it does very simply—and I commend the gentleman from Pennsylvania for the Health Exchange Security and Transparency Act—it accomplishes what this administration has failed to make a standard practice. It will force HHS to inform anyone if their information has been breached, and they have to do this within 2 business days. They can't hide it. They can't spin it. They have got to tell you if your information has been breached.

We do this because if the administration is going to require us—and, yes, to my colleagues, it is a requirement—to use healthcare.gov, at least they can notify you when your information has been breached.

Mr. PALLONE. Mr. Speaker, I yield 3 minutes to the gentlewoman from Texas (Ms. SHEILA JACKSON LEE).

Ms. JACKSON LEE. I thank the distinguished gentleman, and I thank the manager of this legislation, and I thank the good intentions of our colleagues.

I want to pause for a moment, Mr. PALLONE, and just simply say that although these are important issues, as a member of the House Judiciary Committee, I helped draft the PATRIOT Act and business record 215, and we are now looking to constrain the collection of mega-data, and I accept the importance of privacy for the American people. But I pause for just a moment to ask my colleagues, we have enough time today to actually pass the extension of the unemployment benefits. There are 1.3 million people, 12,000 in my own community, who would like us to stay here and make sure that we get that done. I hope that my friends on the other side of the aisle will accept the challenge of Republicans putting an extension of the unemployment benefits on the floor to help unemployed Americans.

But this is an important issue as well, and I do want to say that our friends have not documented any breach on personal and private data of those individuals that have accessed the Affordable Care Act, which are 9 million plus, and growing. We have had 46 votes to repeal it. Now we come one by one with legislation that has not gone through regular order. It has not gone through the committee process. It has very good intentions; but, in actuality, it may be overly burdensome because, Mr. Speaker, there is no bar. There is no limit for HHS to provide notice for any possible breach within seconds or minutes or hours after the incident may have occurred.

Frankly, this legislation doesn't go far enough. Let me give you a few facts. The Affordable Care Act implementation of healthcare.gov is under the authority of HHS. HHS assigned the task for developing healthcare.gov to the agency's Center for Medicare and Medicaid Services. Under the Federal Privacy Act, all Federal agencies must draft regulations to protect personally identifiable information under their control.

The Federal Privacy Act was established by an act of Congress and concurrence of the executive branch to balance the government's need to maintain personal information on Americans with the right of individuals to be protected against unwarranted invasions of their privacy.

The Privacy Act came as a direct result of the work of the Church Committee following revelations that the government has routinely used records on citizens for political purposes to engage in surveillance or retaliatory activity. There were a series of laws

passed by Congress to protect the privacy of Americans.

Computer records management was of such grave concern to Members of Congress following investigations into disclosures that then-President Nixon had used his high office to seek out by means to exact retribution against political enemies by causing harm to careers, reputations as well as financial injury through IRS audits.

The SPEAKER pro tempore. The time of the gentlewoman has expired.

Mr. PALLONE. I yield an additional 1 minute to the gentlewoman.

Ms. JACKSON LEE. So we have had an intense interest since the report ''Records, Computers, and the Rights of Citizens'' was produced in 1973. HHS is chiefly responsible for why the United States became the first Nation in the world to draft a Federal privacy law. They know what to do. They developed the Code of Fair Information practices which have five principles, one of which says there must be no personal data recordkeeping systems whose very existence is secret, that is, to not use the data of people in the wrong way.

There is the CMS Policy for Privacy Act, and I offer this for the RECORD.

The baseline of my point is that HHS was at the core of developing privacy. There have been no known breaches. There is no bar for CMS and HHS to tell the American public or the individual immediately.

This bill will add burdensome requirements and may—it may—distract or take away from legal and lawful law enforcement investigations. I ask that we look at this together in a bipartisan manner. I believe in privacy. I hope we can work together, Mr. PALLONE, and make this what it should be; but I think the American people are protected.

Mr. Speaker, I rise to speak on H.R. 3811, the Health Exchange Security and Transparency Act of 2014.

I would like to commend the author of the bill for the focus on privacy.

Privacy protection is a policy area that has strong bi-partisan agreement.

However, because H.R. 3811 did not go through regular order there was no opportunity for the Committees of jurisdiction to provide valuable input into its drafting.

I would like to offer a few facts that may make it clear that this bill, although well intentioned is not necessary in its current form.

The Affordable Care Act implementation of healthcare.gov is under the authority of the Department of Health and Human Services (HHS).

HHS assigned the task for developing healthcare.gov to the agency's Centers for Medicare & Medicaid Services (CMS).

Under the Federal Privacy Act all federal agencies must draft regulations to protect personally identifiable information under their control.

The Federal Privacy Act was established by an act of Congress and concurrence of the Executive Branch to balance the Government's need to maintain personal information on Americans with the right of individuals to be protected against unwarranted invasions of their privacy.

The Privacy Act came as a direct result of the work of the Church Committee following revelations that the government had routinely used records on citizens for political purposes to engage in surveillance or retaliatory activity a series of laws were passed by Congress to protect the privacy of Americans.

Computer records management was of such grave concern to members of Congress following investigations into disclosures that then President Nixon had used his high office to seek out means to exact retribution against political enemies by causing harm to careers, reputations as well as financial injury through IRS audits.

In 1973, a report ''Records, Computers, and the Rights of Citizens'' was produced by the former Federal Department of Health Education and Welfare (HEW), which today exists as two agencies one of which is the Department of Health and Human Services (HHS) established the first federal agency privacy policies for information held on Americans.

HHS is chiefly responsible for why the United States became the first nation in the world to draft a federal privacy law.

HHS developed the Code of Fair Information practices which later became the basis for the Federal Privacy Act.

The Code of Fair Information Practices has five principles:

There must be no personal data recordkeeping systems whose very existence is secret.

There must be a way for a person to find out what information about the person is in a record and how it is used.

There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.

There must be a way for a person to correct or amend a record of identifiable information about the person.

Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

The Federal Privacy Act protects all personal information managed by Federal agencies.

We know that not all agencies do a good job at protecting the personal information of citizens so today's focus on privacy is relevant and important.

However, our focus should be much broader and better informed regarding the work of each agency in this area.

Committee hearings would have been beneficial in informing the drafters of H.R. 3811, prior to its introduction on the Floor of the House for a vote.

For example, authors of the bill may have taken a different approach if it was acknowledged that the CMS has several policy documents specific to the topic of protecting personal identifiable information of medical records data:

CMS Policy for Privacy Act Implementation & Breach Notification (7/23/07)

Risk Management Handbook Volume III Standard 7.1 (12/6/12)

Incident Handling and Breach Notification

CMS Privacy Policy is written to meet obligations established by the Federal Privacy Act of 1974 (5 U.S.C., 552a), the Computer Matching and Privacy Protection Act of 1988 (Public Law 100–503) and the Department of Health and Human Services Privacy Act Regulations (45 C.F.R. Part 5b).

I want to assure my colleagues that under the Federal Privacy Act all Federal agencies must ''develop an effective response to [breaches] that requires disclosure of information regarding the breach to those individuals affected by it, as well as to persons and entities in a position to cooperate, either by assisting in notification to affected individuals or playing a role in preventing or minimizing harms from the breach.''

All agencies, which include CMS, must report all incidents involving personally identifiable information to US-Computer Readiness Team or (US-CERT).

The US-CERT reporting requirement does not distinguish between potential and confirmed breaches—all must be reported within 1 hour of discovery/detection.

The CMS policy on breach notification has 5 criteria to determine if a breach has occurred:

Nature of the Data Elements Breached

Number of Individuals Affected

Likelihood the Information is Accessible and Usable

Likelihood the Breach May Lead to Harm

Ability of the Agency to Mitigate the Risk of Harm

CMS is directed to provide notification without unreasonable delay following the discovery of a breach, consistent with the needs of law enforcement and any measures necessary for CMS to determine the scope of the breach and, if necessary, to restore the integrity of the computerized system.

The consideration of Law-enforcement in government agency breaches is very important because this type of crime can take place in seconds or it may occur over hours, days, weeks or months.

Law-enforcement in investigation of data breaches attempts to identify the culprit(s) and others who may be involved.

To avoid impeding the efforts of law-enforcement or national security H.R. 3811, the Health Exchange Security and Transparency Act of 2014 should have included a law-enforcement exception.

Responsibility for information on individuals whose personally identifiable information has been breached is the CMS Administrator the highest official of the agency.

However, if the data breach is under 50, the notice may also be issued by the CMS Chief Information Officer or Senior Official for Privacy.

CMS Breach Notification to individuals must be in writing that should be ''concise, conspicuous, and in plain language'' and include the following:

Brief description of what happened, including date(s) and its discovery;

Description of the types of information involved in the breach;

Whether the information was encrypted or protected by other means when determined the information may be useful or compromise the security of the system;

What steps individuals should take to protect themselves from potential harm;

What the agency is doing; and

Who affected individuals should contact

There is no evidence that healthcare.gov had a breach of personal information.

If such a breach had occurred it would not be secret and members of this body would have been briefed.

First, the most important rule for cyber security is following the example of the professionals who work in this fast paced area: truth comes before beauty. The truth is that there is no computer system that is 100 percent secure from hostile cyber attacks, natural disasters, structural failures or human errors.

Second, the Internet is a rough neighborhood—the best we can do is to design the best systems possible provide the resources necessary to follow through on good security and privacy designs and ignore the politics of the moment. The most dangerous threats to cyber security do not care about anyone's political party they may care very much about your nation of origin.

Third, cyber security is not about the 14 year old with a laptop, but the botnet attack from a coordinate effort that brings to the discussion significant threats to networks. There is no evidence that nothing occurred that would suggest that the website experienced anything of this nature.

Congress should use regular order to consider means and methods of securing all federal data that is categorized as personally identifiable information.

Attempts to misinform or frighten Americans regarding the healthcare.gov or the Patient Protection and Affordable Care Act implementation mechanisms are unwarranted.

CMS has a detailed and well managed program for ensuring that personally identifiable information is secure and when questions arise they have a top level ''Incident Handling'' protocol that is through in investigating issues and uncovering the facts regarding suspected breaches.

CMS relies upon US-CERT, which is part of DHS' National Cybersecurity and Communications Integration Center (NCCIC) to address breaches of data it manages.

The Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) leads efforts to improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the Nation while protecting the constitutional rights of Americans.

CMS informs US-CERT within an hour of a suspected breach incident.

However, a report does not mean that an incident occurred an investigation must proceed to determine if the report is valid.

It is important note that premature breach notices being sent to consumers regarding their personally identifiable information could have unintended and adverse outcomes for several reasons:

Notice fatigue—too many notices and people stop paying attention;

Increased cost of administering a program due to additional communications that inform people that the initial breach notice was a false alarm;

Giving notice to cyber criminals or terrorists that they have been discovered before law enforcement or national security can assess how the extent of the threat, the target or objective of the attack and trace the source of the threat with the goal of identifying the culprits; and

Correcting the problem that allowed the breach to occur

HHS should only collect the personally identifiable information that is necessary, used it for the purpose of the collection and promptly discarded that data so no database or system of records is created.

I commend my colleagues for the focus on Privacy and hope that we can work together to improve the protection of personal information on Americans throughout the Federal Government.

I strongly recommend that my colleagues vote to send this bill back for committee consideration so that its goal of improving privacy protection can be better matched to the reality of what CMS is currently doing in the area of breach notification, which conforms to what Americans need and law-enforcement as well as national security must have to protect federal agency computer networks.

1 INTRODUCTION

CMS must be able to respond to computer security-related and/or privacy-related incidents in a manner that protects its own information and helps to protect the information of others that might be affected by the incident.

This Risk Management Handbook Volume III, Standard 7.1, Incident Handling and Breach Notification standard, along with the companion procedures of the RMH Volume II, Procedure 7.2, Incident Handling, supersedes the CMS Information Security (IS) Incident Handling and Breach Analysis/Notification Procedure dated December 3, 2010.

1.1 Background

1.1.1 SECURITY EVENT

A Security Event is an observable occurrence in a network or system (e.g., known or suspected penetrations of information Technology (IT) resources, probes, infections, log reviews), or any occurrence that potentially could threaten CMS data confidentiality, integrity, or availability.

1.1.2 REPORTABLE EVENT

A Reportable Event is any activity or occurrence that involves:

A matter that a reasonable person would consider a violation of criminal, civil, or administrative laws applicable to any Medicare contract or federal health care program.

Integrity violations, including any known, probable, or suspected violation of any Medicare contract term or provision.

A matter considered to have an ''adverse'' impact on the IT system/infrastructure or CMS data confidentiality, integrity, or availability. Examples of specific events that should be reported include (but are not limited to):

Unauthorized access to or use of sensitive data for illegal purposes.

Unauthorized altering of data, programs, or hardware.

Loss of mission-essential data (i.e., patient, financial, benefits, legal, etc.).

Environmental damage/disaster (greater than $10,000) causing loss of IT services or data, or which may be less than $10,000 in damage yet affect CMS' ability to continue any day-to-day functions and operations.

Infection of sensitive systems, firmware, or software by malicious code (i.e., Viruses, Worms and Trojan Horses, etc.).

Perpetrated theft, fraud, vandalism, and other criminal computer activity that did, or may, affect the organization's capabilities to continue day-to-day functions and operations.

Telecommunications/network security violations, i.e., networks (including local area networks [LANs], metropolitan area networks [MANs], and wide area networks [WANs]) that experience service interruptions that cause an impact to an indefinite number of end users.

Unauthorized access to data when in transmission over communications media.

Loss of system availability affecting the ability of users to perform the functions required to carry out day-to-day responsibilities.

Root-level attacks on networking infrastructure, critical systems, or large, multipurpose, or dedicated servers.

Compromise (or disclosure of account access information) of privileged accounts on computer systems.

Compromise (or disclosure of account access information) of individual user accounts or desktop (single-user) systems.

Denial-of-service attacks on networking infrastructure and systems.

Attacks launched on others from within organizational boundaries or systems.

Scans of internal organizational systems originating from the Internet or from within the organizational boundaries.

Any criminal act that may have been committed using organizational systems or resources.

Disclosure of protected data, including paper disclosure, email release, or inadvertent posting of data on a web site.

Suspected information-technology policy violation.

A Reportable Event may be the result of an isolated event or a series of occurrences. Reportable Events under these procedures include events that occur at CMS federal sites, contractor/subcontractor sites/systems, consultants, vendors or agents. If the Reportable Event results in an overpayment relating to either Trust Fund payments or administrative costs, the report must describe the overpayment with as much specificity as possible, as of the time of the due date for the submission of the report.

Security events that may consist of an observable occurrence in a network or system (e.g., detected probes, infections prevented, log reviews, etc.), that do not threaten system integrity, are not considered Reportable Events unless they may be reasonably associated with other incidents, Reportable Events, or breaches. CMS categorizes these events in a monthly report to the Department of Health and Human Services (HHS) (hereafter referred to as the ''Department'' or ''HHS'') Cybersecurity Program as follows:

Malicious Code Prevented: Viruses were prevented and did not cause any harm to any system.

Probes and Reconnaissance Scans Detected: Probes and scans were detected but did not pose a serious threat to a CMS system.

Inappropriate Usage: Misuse of computing resources by an otherwise authorized individual.

Other: Cannot be categorized under any of the above and do not threaten system integrity.

There are many events that may be flagged as inappropriate use of resources, but reflect situations that do not fall under the definitions associated with incidents, Reportable Events, or breaches. In such cases, reporting should be made through applicable contractual resources, or through appropriate Federal Fraud, Waste, and Abuse reporting channels.

1.1.3 PRIVACY INFORMATION

Privacy is the right of an individual to control their own personal information, and not have it disclosed or used by others without permission. At CMS, we are charged with protecting other people's private information—that of every citizen (or legal resident) beneficiary utilizing benefits the vast Medicare/Medicaid program, as well as many subsidiary programs.

Confidentiality is the obligation of another party to respect privacy by protecting personal information they receive, and preventing it from being used or disclosed without the subject's knowledge and permission.

Again, at CMS we are charged with protecting the confidentiality of other people's citizen-beneficiary information. A breach of that confidentiality is not simply a failure of a ''technical control'', it is a basic failure of CMS to meet its obligation to protect the individual citizen. Moreover, unlike the banking industry where financial compensation is a readily-available remedy to a breach, private medical information cannot be simply replaced with something of ''similar value'', or by simply closing an account, and opening a new (better protected) one. Once a privacy breach occurs, the ramifications can be far-reaching and long lasting—with no readily available ''patch'' to undo the damage (we cannot simply replace one violated health record with a brand new one.)

Security is the means used to protect the confidentiality of personal information through physical, technical, and administrative safeguards.

Privacy is the ''business objective'' of security. The core of the relationship between information security and information privacy lies in the fact that security, or lack of it, is the determinant of the level of privacy that a system or infrastructure can assure. If there is a breach of computer security, it has a corresponding negative effect on the confidentiality, integrity, and availability of the information therein. Inadequate security leads directly to loss of privacy. Therefore, if privacy is the ''business objective'', then security is the ''functional requirements'' necessary for an IT system to meet those ''business objectives''.

1.1.3.1 PERSONALLY IDENTIFIABLE INFORMATION (PII)

Personally Identifiable Information (PII) is information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. PII also includes individually identifiable health information as defined by the Health Insurance Portability and Accountability Act (HIPAA) of 1996, Privacy Rule (45 CFR Section 164.501. PII is also often referred to as personally identifiable data or individually identifiable information.

1.1.3.2. PROTECTED HEALTH INFORMATION (PHI)

Protected Health Information (PHI) is individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.

Individually Identifiable Health Information is a subset of health information, including demographic data collected concerning an individual that:

Is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse.

Relates to the past, present or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual, and meets either of the following:

Identifies the individual.

There is a reasonable basis to believe the information can be used to identify the individual.

The HIPAA Privacy Rule excludes from the definition of PHI individually identifiable health information that is maintained in education records covered by the Family Educational Right and Privacy Act (as amended, 20 U.S.C. 1232g) and records described at 20 U.S.C. 1232g(a)(4)(B)(iv), and employment records containing individually identifiable health information that are held by a covered entity in its role as an employer.

The HIPAA Privacy Rule covers PHI in any medium (including paper) while the HIPAA Security Rule covers PHI in electronic form (ePHI) only.

1.1.3.3 DE-IDENTIFIED HEALTH INFORMATION

With those definitions in place, what information (or data) elements comprise PHI such that, if they were removed, the above definition of individually identifiable health information would not apply? The answer is in the HIPAA de-identification use standard and its two implementation specifications of the HIPAA Privacy Rule.

There are no restrictions on the use or disclosure of de-identified health information. De-identified health information neither identifies nor provides a reasonable basis to identify an individual. There are two specifications for de-identifying individually identifiable health information; either: 1) a formal determination by a qualified statistician; or 2) the removal of specified identifiers of the individual and of the individual's relatives, household members, and employers is required, and is adequate only if the covered entity has no actual knowledge that the remaining information could be used to identify the individual.

The following identifiers of the individual or of relatives, employers, or household members of the individual must be removed to achieve the safe harbor method of de-identification:

1. Names
2. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of Census:

a. The geographic units formed by combining all zip codes with the same three initial digits contains more than 20,000 people.

b. The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

3. All elements of dates (except year) for dates directly related to the individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
4. Telephone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voiceprints
17. Full face photographic images and any comparable images.
18. Any other unique identifying number, characteristic, or code, except as permitted for re-identification purposes provided certain conditions are met

In addition to the removal of the above-stated identifiers, the covered entity may not have actual knowledge that the remaining information could be used alone or in combination with any other information to identify an individual who is subject of the information.

Mr. PITTS. Mr. Speaker, at this time I am pleased to yield 1 minute to the gentleman from Louisiana (Mr. SCALISE), the distinguished chairman of the Republican Study Committee and a member of the Energy and Commerce Committee.

Mr. SCALISE. I thank the gentleman from Pennsylvania for yielding and for bringing the Health Exchange Security and Transparency Act. Mr. Speaker, all we are saying here is if American families' personal information is stolen through this Web site, through the exchange Web site, they ought to be notified by the administration that their data was breached.

And, of course, you have the White House actually coming out and saying they will veto this bill. What does the Obama administration have against protecting the privacy of American families' personal information? You have got an administration official who testified for our committee, the chief information security officer who actually said there is also no confidence that personal identifiable information will be protected.

Well, if they can't ensure the protection—and by the way, the individual mandate says this is not an option for American families, they have to go through this exchange to get insurance that is approved by the government. So if the government is going to mandate it, and we don't want the government to mandate this, but if they are going to mandate it, they ought to be able to ensure that the data is protected. And if it is breached, they ought to notify them that this has happened. And yet they issue a veto threat against this. We need to pass this legislation and put this transparency in law. Pass this bill.

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

Mr. Speaker, once again I hear my colleagues on the other side repeating the same things that are not accurate. You do not have to go on healthcare.gov to sign up for health insurance. Mr. WAXMAN said you can go to a private insurance broker or call an 800 number. You can go through various nonprofits. They keep repeating the same thing, and we keep having to say that there have been no breaches.

The gentleman mentioned the administration. The administration statement, which I read before and I will only summarize part of it now, it says that the Federal Government has already put in place an effective and efficient system for securing personally identifiable information in the health insurance marketplace. The administration opposes the bill because it would create unrealistic and costly paperwork requirements that do not improve the safety or security of personally identifiable information in the health insurance marketplace. The purpose of the bill I understand; but it is simply not necessary, and it is just making people fearful of signing up.

I reserve the balance of my time.

Mr. PITTS. Mr. Speaker, I yield 1 minute to the gentleman from Colorado (Mr. GARDNER).

□ 1015

Mr. GARDNER. I thank the chairman of the committee for his good work.

Mr. Speaker, I would remind our colleagues that when you call the 800 number to sign up for the exchange policies, as was heard before our committee in testimony, the people who get that number on that phone call then turn around and use the healthcare.gov site—the information, the Web site—to input that information. So you are forced to go through this site.

A couple of weeks ago I received this letter:

> We are writing to you because an electronic file containing your personal information cannot be accounted for. The file included two or more of the following: your name, home mailing address, and Social Security number.

The letter went on to say:

> We wanted to alert you to the potential that someone not authorized to access the records could have seen the information.

This letter came from the State of Colorado, this letter from the State of Colorado because they couldn't hold on to State employees' private personal identification information.

All we are asking for is that we protect the privacy, the security of the American people. To oppose this bill, to issue a veto threat, if the site is secure, they will never receive the notice; if it is not, we will have acted to protect the American people.

STATE OF COLORADO,
Yuma, CO.

MR. GARDNER: We are writing to you because an electronic file containing your personal information cannot be accounted for. The file included two or more of the following: your name, home/mailing address and Social Security number.

There is no indication that your information has been misused or stolen, and we are continuing efforts to account for the file. Still, we wanted to alert you to the potential that someone not authorized to access the records could have seen the information, although that is unlikely.

As a precaution, we recommend that you visit the Colorado Attorney General's Office's website at http://www.colorado attorneygeneral.gov/initiatives/identity __theft, which contains information on how to protect yourself from the possibility of identity theft. Once again, we do not have any indication that your information has been misused or stolen and believe such misuse is unlikely.

We deeply regret that this incident occurred. We want to assure you that we are reviewing and revising our procedures and practices to minimize the risk of recurrence. Should you need any further information, please contact the Office of Information Security at infosec@state.co.us.

Sincerely,

JONATHAN C. TRULL,
Chief Information Security Officer.

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

Mr. PITTS. Mr. Speaker, I am pleased to yield 1 minute to the gentleman from Ohio (Mr. JORDAN).

Mr. JORDAN. Mr. Speaker, the independent contractor said they were unable to adequately test the confidentiality and integrity of the system. They said no complete end-to-end testing was done. The chief information security officer recommended not launching it, her boss refused to sign the authority to operate, and they launched it anyway. They knew, the administration knew this Web site wasn't ready; they launched it anyway. The whole country now knows it wasn't ready. They launched it anyway, put millions of people's personal information at risk, and they did it for political reasons.

Now all we are asking—all we are asking—is when there is a breach, when there is a problem, at least tell the American citizens. You already launched a Web site for political reasons that you knew wasn't ready, put millions of Americans' personal information at risk. You already did that. Now we are saying, if there is a problem, at least tell them. That is all this bill does.

And what does the administration say? We are going to veto that bill if it happens.

You have got to be kidding me. You have got to be kidding me. That is all this is about.

So I want to commend Mr. PITTS, the committee, and those individuals who put work into this. It is a good piece of legislation, and I would urge a ''yes'' vote.

Mr. PALLONE. Mr. Speaker, I continue to reserve the balance of my time.

Mr. PITTS. Mr. Speaker, at this time, I am pleased to yield 1 minute to the gentlelady from Kansas (Ms. JENKINS), the distinguished secretary of our caucus.

Ms. JENKINS. Mr. Speaker, I thank the gentleman for yielding.

Health care is a personal issue, and many Kansans are worried about submitting their sensitive and private information into a system that can't protect them against the devastating consequences of security breaches and fraud.

Experts have repeatedly raised red flags about the security of the information people are submitting to the ObamaCare exchanges, and a former Social Security Administrator even described the Web site as a hacker's dream. Important questions about the Web site security remain unanswered, and Americans, especially those who have lost their plans due to the President's health care law, deserve some piece of mind that their information is safe from cyber thieves.

I urge my colleagues to support this bill that requires HHS to notify Americans within 2 business days if their personal information has been compromised. Much more is required of private sector companies whose products are not mandated by law. The least the administration can do is notify Americans if their information has been stolen or unlawfully accessed through the ObamaCare exchange.

Mr. PALLONE. Mr. Speaker, I continue to reserve the balance of my time.

Mr. PITTS. Mr. Speaker, at this time, I am pleased to yield 1 minute to the gentlelady from Indiana (Mrs. WALORSKI).

Mrs. WALORSKI. Mr. Speaker, I am pleased to cosponsor this legislation to enact much-needed consumer protections for healthcare.gov.

It is unfair that the Department of HHS launched healthcare.gov without performing a complete security control assessment. Installing the necessary safeguards for the exchanges should have been the administration's top priority.

Now Congress has an opportunity to pass a law that simply requires HHS to notify consumers within 2 business days if their personal information is unlawfully accessed or stolen. In a digital world, Americans deserve to know their information is compromised so they can immediately take action to protect themselves.

Last summer, I traveled my entire district in Indiana to notify and to make aware cybersecurity issues and steps to avoid identity theft. Hoosiers in Indiana, especially seniors, shared with me frightening stories about fraud and scams. They need to know that healthcare.gov will not contribute to the cybersecurity dilemma. This is the kind of representation they deserve in Congress.

I urge my colleagues to support this commonsense law to safeguard our personal information.

Mr. PALLONE. Mr. Speaker, I continue to reserve the balance of my time.

Mr. PITTS. Mr. Speaker, we are prepared to close, and I reserve the balance of my time.

Mr. PALLONE. Mr. Speaker, I just want to say, again, I am not saying that I am opposed to some kind of security notification. In fact, it already exists and there is a protocol in place with the Department of Health and Human Services. The point is that this Republican bill is simply not necessary. That security already exists.

The fact of the matter is there have not been any security breaches. Once again, we are simply seeing the Republicans get up and try to scare people so that they don't go and use healthcare.gov, the Web site.

What we would really like to see, Mr. Speaker, is the day when, on both sides of the aisle here, we can simply get up and talk about legislation that continues to provide outreach and encourage people to sign up for the Web site and get the health insurance that they need. I still honestly believe that most Republicans and Democrats collectively would like to see most Americans covered with health insurance. That was the purpose of the Affordable Care Act.

I think my one optimistic note today could be at least we are not seeing another bill on the floor that would seek to repeal the Affordable Care Act. Hopefully, that is some recognition on the Republican side that the Affordable

Care Act is actually accomplishing its goal of trying to cover most Americans, if not all Americans.

With that, Mr. Speaker, I urge my colleagues to oppose this unnecessary bill, and I yield back the balance of my time.

Mr. PITTS. Mr. Speaker, some have argued that requiring HHS to report a data breach that is known to have resulted in a loss of personal identifiable information within 2 days is too burdensome for the Department. In fact, the administration opposes this legislation for ''paperwork requirements.''

I am frankly shocked that any Member of this body would put workload concerns of HHS ahead of their constituents' right to know if their data has been breached when many of our constituents are essentially being forced to shop through these exchanges.

In addition, CMS has stated that States and other nonexchange entities are required to report data breaches to the Department within 1 hour to HHS. If HHS believes 1 hour is enough time to report, then they should certainly be able to tell our constituents within 2 days after knowing an individual's information was breached through an exchange.

Our constituents deserve to know if their personal information has been breached. That is all the underlying bill requires. Our constituents have a right to know. They should have peace of mind, and we should be protecting them, the victims, not the bureaucracy.

I urge my colleagues to support this commonsense, important bill, and I yield back the balance of my time.

Mr. DEFAZIO. Mr. Speaker, I will vote for H.R. 3811 with significant reservations. There is no question that Americans must be quickly notified if their personal information on Healthcare.gov or a state exchange website is compromised. Current law accomplishes this without a hard and fast deadline. H.R. 3811 aims to add a hard deadline for notification, and that is why I voted for it. Unfortunately the bill is poorly drafted. H.R. 3811 fails to provide any delay for public disclosure if immediate disclosure would derail a federal investigation. Americans have a right to know if their personal information has been stolen or misused, but it is also critical that our federal law enforcement agencies be able to hunt down and prosecute those responsible for a data breach. Republicans need to work with the Administration and Democrats in Congress to come up with a bipartisan solution that makes sure that enforcement can do their job and establishes prompt but reasonable disclosure requirements to protect consumers.

Mr. BLUMENAUER. Mr. Speaker, we are in a new year, and a new session. The Affordable Care Act is the law of the land, and we should find a way to move past this empty, meaningless bickering.

I will vote against H.R. 3811 because this bill is a diversion tactic by the Republicans, designed to scare Americans away from obtaining affordable health coverage and further undermines confidence in Government.

This bill serves no useful purpose. The mere fact that this bill is only directed at the Department of Health and Human Services (HHS), and no other agency that handles personally identifiable information, demonstrates that Republicans are only attacking the Affordable Care Act for political purposes; not to make it work better to give Americans the health care they are entitled to under the law.

Not only is this bill a waste of time, but it detracts from the real work we need to do to strengthen our health care system. If my colleagues were serious about improving the Affordable Care Act, we'd welcome that discussion, but to date the only interest they have is frightening Americans away from a law that would provide the affordable, accessible health coverage to those who need it most.

Just this week, the Centers for Medicare and Medicaid Services (CMS) announced that the increase in overall health care costs for the last four years is the lowest we've ever recorded in part as a result of the reforms taking place. We should be focused how to build on and take advantage of that trend, for example repealing the flawed and burdensome Medicare sustainable growth rate (SGR) and avoid the ordeal we subject the health care community to every year.

Please let's stop this senseless exercise in futility and work together for a more productive 2014 and effectively provide the healthcare Americans are entitled to under the Law.

Mr. DINGELL. Mr. Speaker, I rise in opposition to H.R. 3811, the Health Exchange Security and Transparency Act.

There is a very real and pressing need for Congress to enact data security and breach notification requirements. But H.R. 3811 isn't the way to do it. At only a paragraph long, the bill is vague, far too limited in scope and, quite frankly, absolutely unworkable. It fails to define what constitutes ''personally identifiable information,'' a key component to any successful data security and breach-bill. It applies only to the Affordable Care Act and has no bearing on the sorts of massive breaches like the one Target just reported. And its 48-hour notification requirement would impede accurate reporting to consumers about whose and what information has been breached.

Mr. Speaker, H.R. 3811 isn't meant to solve a problem. It's another attempt by my Republican friends to throw egg on the Administration's face. Our consideration of this bill is also an affront to regular order because H.R. 3811 hasn't even been considered by the Committee on Energy and Commerce. That said, data security and breach notification legislation is absolutely necessary. If my friends on the other side of the aisle are truly willing to work on comprehensive bipartisan legislation, they'll find a willing partner in me. But they have to stop with cynical, politically motivated half-measures and genuinely commit to protecting the interests of consumers.

Vote down this bill.

Mr. SMITH of Texas. Mr. Speaker, when the Obama Administration launched Healthcare.gov, Americans were led to believe that the website was safe and secure. As the Science, Space, and Technology Committee learned at our hearing in November, this was not the case.

Healthcare.gov comprises one of the largest collections of personal information ever assembled.

The Administration has a responsibility to ensure that Americans' personal and financial data is secure. And individuals should be notified when their personal information has been compromised.

Instead, the Centers for Medicare and Medicaid Services chose not to notify individuals when a security breach occurs.

This bill makes sure that individuals get the information they need to protect themselves.

By alerting users when a security breach occurs on the ObamaCare website, they can take action to limit the consequences.

If the Administration won't protect the privacy and security of Americans, then Congress should.

The SPEAKER pro tempore. All time for debate has expired.

Pursuant to House Resolution 455, the previous question is ordered on the bill.

The question is on the engrossment and third reading of the bill.

The bill was ordered to be engrossed and read a third time, and was read the third time.

The SPEAKER pro tempore. The question is on the passage of the bill.

The question was taken; and the Speaker pro tempore announced that the ayes appeared to have it.

Mr. PALLONE. Mr. Speaker, on that I demand the yeas and nays.

The yeas and nays were ordered.

The vote was taken by electronic device, and there were—yeas 291, nays 122, not voting 19, as follows:

[Roll No. 11]

YEAS—291

Aderholt	Costa	Griffin (AR)
Amash	Cotton	Griffith (VA)
Amodei	Cramer	Grimm
Bachmann	Crawford	Hahn
Bachus	Crenshaw	Hall
Barber	Cuellar	Hanabusa
Barletta	Culberson	Hanna
Barr	Daines	Harper
Barrow (GA)	Davis, Rodney	Harris
Barton	DeFazio	Hartzler
Benishek	Delaney	Hastings (WA)
Bentivolio	Denham	Hensarling
Bera (CA)	Dent	Himes
Bilirakis	DeSantis	Holding
Bishop (NY)	DesJarlais	Horsford
Bishop (UT)	Diaz-Balart	Hudson
Black	Doggett	Huelskamp
Blackburn	Duckworth	Huizenga (MI)
Boustany	Duffy	Hultgren
Brady (TX)	Duncan (SC)	Hunter
Braley (IA)	Duncan (TN)	Hurt
Bridenstine	Ellmers	Israel
Brooks (AL)	Enyart	Issa
Brooks (IN)	Esty	Jenkins
Broun (GA)	Farenthold	Johnson (OH)
Brownley (CA)	Fincher	Johnson, Sam
Buchanan	Fitzpatrick	Jordan
Bucshon	Fleischmann	Joyce
Burgess	Fleming	Kaptur
Bustos	Flores	Keating
Byrne	Forbes	Kelly (PA)
Calvert	Fortenberry	Kilmer
Camp	Foster	King (IA)
Campbell	Foxx	King (NY)
Cantor	Franks (AZ)	Kingston
Capito	Frelinghuysen	Kinzinger (IL)
Capps	Gallego	Kirkpatrick
Capuano	Garamendi	Kline
Carney	Garcia	Kuster
Cartwright	Gardner	Labrador
Cassidy	Garrett	LaMalfa
Chabot	Gerlach	Lamborn
Chaffetz	Gibbs	Lance
Cicilline	Gibson	Langevin
Coble	Gingrey (GA)	Lankford
Coffman	Gohmert	Latham
Cole	Goodlatte	Latta
Collins (GA)	Gosar	Lipinski
Collins (NY)	Gowdy	LoBiondo
Conaway	Granger	Loebsack
Connolly	Graves (GA)	Lofgren
Cook	Graves (MO)	Long

Lucas
Luetkemeyer
Lujan Grisham (NM)
Luján, Ben Ray (NM)
Lummis
Lynch
Maffei
Maloney, Carolyn
Maloney, Sean
Marchant
Marino
Massie
Matheson
McAllister
McCarthy (CA)
McCaul
McHenry
McIntyre
McKeon
McKinley
McMorris Rodgers
Meadows
Meehan
Messer
Mica
Michaud
Miller (FL)
Miller (MI)
Miller, Gary
Mullin
Mulvaney
Murphy (FL)
Murphy (PA)
Neugebauer
Noem
Nolan
Nugent
Nunes
Nunnelee
Olson
Owens
Palazzo
Paulsen
Pearce
Perry
Peters (CA)
Peters (MI)
Peterson
Petri
Pingree (ME)
Pittenger
Pitts
Poe (TX)
Pompeo
Posey
Price (GA)
Radel
Rahall
Reed
Reichert
Renacci
Ribble
Rice (SC)
Rigell
Roby
Roe (TN)
Rogers (AL)
Rogers (KY)
Rogers (MI)
Rohrabacher
Rokita
Rooney
Ros-Lehtinen
Roskam
Ross
Rothfus
Royce
Runyan
Ryan (WI)
Salmon
Sanford
Scalise
Schneider
Schock
Schrader
Schwartz
Schweikert
Scott, Austin
Sensenbrenner
Sessions
Shea-Porter
Sherman
Shimkus
Shuster
Simpson
Sinema
Smith (MO)
Smith (NE)
Smith (NJ)
Smith (TX)
Southerland
Speier
Stewart
Stivers
Stutzman
Terry
Thompson (PA)
Thornberry
Tiberi
Tierney
Tipton
Titus
Turner
Upton
Valadao
Vela
Wagner
Walberg
Walden
Walorski
Walz
Weber (TX)
Wenstrup
Westmoreland
Whitfield
Williams
Wilson (SC)
Wittman
Wolf
Womack
Woodall
Yoder
Yoho
Young (AK)
Young (IN)

NAYS—122

Andrews
Bass
Beatty
Becerra
Bishop (GA)
Blumenauer
Bonamici
Brady (PA)
Brown (FL)
Butterfield
Cárdenas
Carson (IN)
Castor (FL)
Castro (TX)
Chu
Clark (MA)
Clarke (NY)
Clay
Clyburn
Cohen
Conyers
Courtney
Crowley
Cummings
Davis (CA)
Davis, Danny
DeGette
DeLauro
DelBene
Deutch
Dingell
Doyle
Edwards
Ellison
Engel
Eshoo
Farr
Fattah
Frankel (FL)
Fudge
Grayson
Green, Al
Green, Gene
Grijalva
Gutiérrez
Hastings (FL)
Heck (WA)
Higgins
Hinojosa
Holt
Honda
Hoyer
Huffman
Jackson Lee
Jeffries
Johnson (GA)
Johnson, E. B.
Kelly (IL)
Kennedy
Kildee
Kind
Larsen (WA)
Larson (CT)
Lee (CA)
Levin
Lewis
Lowenthal
Lowey
Matsui
McCollum
McDermott
McGovern
McNerney
Meeks
Meng
Miller, George
Moore
Moran
Nadler
Napolitano
Negrete McLeod
O'Rourke
Pallone
Pascrell
Pastor (AZ)
Payne
Pelosi
Pocan
Polis
Price (NC)
Quigley
Rangel
Richmond
Roybal-Allard
Ryan (OH)
Sánchez, Linda T.
Sanchez, Loretta
Sarbanes
Schakowsky
Schiff
Scott (VA)
Scott, David
Serrano
Sewell (AL)
Sires
Swalwell (CA)
Takano
Thompson (CA)
Thompson (MS)
Tonko
Tsongas
Van Hollen
Vargas
Veasey
Velázquez
Visclosky
Wasserman Schultz
Waters
Waxman
Welch
Wilson (FL)
Yarmuth

NOT VOTING—19

Carter
Cleaver
Cooper
Gabbard
Guthrie
Heck (NV)
Herrera Beutler
Jones
McCarthy (NY)
McClintock
Neal
Perlmutter
Ruiz
Ruppersberger
Rush
Slaughter
Smith (WA)
Stockman
Webster (FL)

□ 1054

Messrs. LYNCH and SAM JOHNSON of Texas, Ms. HAHN, Mr. CICILLINE, Ms. SPEIER, and Mr. LANGEVIN changed their vote from ''nay'' to ''yea.''

So the bill was passed.

The result of the vote was announced as above recorded.

A motion to reconsider was laid on the table.

Stated for:

Mr. WEBSTER of Florida. Mr. Speaker, on rollcall No. 11, had I been present, I would have voted "yes."

PERSONAL EXPLANATION

Mr. CLEAVER. Mr. Speaker, due to a medical procedure, I was unable to vote the week of January 7th. On Tuesday, January 7, I would have voted "present" on rollcall vote No. 1 (Quorum).

On January 8, I would have voted "yes" on rollcall vote No. 2 (H.R. 721), "yes" on rollcall vote No. 3 (H.R. 3527), and "yes," on rollcall vote No. 4 (H.R. 3628).

On January 9, I was also unable to vote. Had I been present, I would have voted "no" on rollcall vote No. 5 (Ordering the Previous Question), "no" on rollcall vote No. 6 (H. Res. 455), "yes" on rollcall vote No. 7 (Sinema Amendment No. 1), "yes" on rollcall vote No. 8 (Tonko Amendment No. 2), "yes" on rollcall vote No. 9 (Motion To Recommit with Instructions), and "no" on rollcall vote No. 10 (Final Passage of H.R. 2279).

On January 10, I would have voted "no" on rollcall vote No. 11 (Final Passage of H.R. 3811).

REMOVAL OF NAME OF MEMBER AS COSPONSOR OF H.R. 3550

Mr. MEADOWS. Mr. Speaker, I ask unanimous consent to remove my name as a cosponsor from H.R. 3550.

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

There was no objection.

LEGISLATIVE PROGRAM

(Mr. HOYER asked and was given permission to address the House for 1 minute.)

Mr. HOYER. Mr. Speaker, I yield to my friend, Mr. CANTOR, for the purpose of inquiring of the majority leader the schedule for the week to come.

Mr. CANTOR. Mr. Speaker, I thank the gentleman from Maryland, the Democratic whip, for yielding.

Mr. Speaker, on Monday, the House will meet at noon for morning-hour and 2 p.m. for legislative business. Votes will be postponed until 6:30 p.m. On Tuesday and Wednesday, the House will meet at 10 a.m. for morning-hour and noon for legislative business. On Thursday, the House will meet at 9 a.m. for legislative business. Last votes of the week are expected no later than 3 p.m. On Friday, no votes are expected.

Mr. Speaker, the House will consider a few suspensions next week, a complete list of which will be announced by the close of business today. In addition, the House will consider two bills next week to fund government operations.

As you know, Mr. Speaker, House and Senate appropriators are working towards a bipartisan agreement on an appropriations package to fund the government for the remainder of the fiscal year. I expect an agreement to be reached soon. The House will consider this package next week.

Mr. Speaker, to facilitate this, we will need to pass a short-term CR to allow the Senate time to process the bill. I expect to pass this under suspension of the rules early next week.

Finally, I expect the House to consider H.R. 3362, the Exchange Information Disclosure Act, sponsored by Representative LEE TERRY. This bill requires full transparency and accuracy from the administration on data reported from the ObamaCare exchange.

□ 1100

Mr. HOYER. I thank the gentleman for that information. I note that he indicates that we probably will not be able to accomplish the omnibus by the end of next week and, therefore, a CR may be required.

I know that all of us feel that that needs to be accomplished as quickly as possible. I would point out to the gentleman in conversations that he says it is going to be on suspension. I will support it on suspension, urge my colleagues to support it on suspension.

Can the gentleman tell me, however, how long that CR will go that will affect us somewhat?

Mr. CANTOR. Mr. Speaker, I would say to the gentleman in response to his question, the expected termination, if you will, expiration of the CR will be Saturday, January 18. So giving a week really, Mr. Speaker, for the Senate to act, because we will be acting next week in the middle of the week. We hope that they will finish their business by September—I mean January 18.

Mr. HOYER. I hope that was not a Freudian slip of our confidence in the ability to get that done as quickly as we would like.

In any event, I think that is appropriate, and I am hopeful that we can, in fact, accomplish that.

I want to tell the majority leader from my perspective that if we don't get that done in the short term, then I would be very reluctant to support continuing resolutions at the level which has now been substituted for the agreement that was reached in the bipartisan budget agreement.

There are substantial differences, as you know, in the 302(a) allocation, the allocation of discretionary spending, one at $1.012 trillion and one at $986 billion, so that there is a substantial discrepancy between those figures.

We reached agreement on the higher number. The Senate came down about 45, the House went up about 45 and reached a compromise. I think America was pleased that we reached a compromise. I would want to be on the