Mr. BISHOP of Utah. Mr. Speaker, switching gears to the intelligence re-authorization measure, every Member of the House takes seriously our responsibility to preserve individual liberty and freedoms under the Constitution.

We also have a constitutional obligation to provide for the common defense, because without a strong national defense, which includes the indispensable work of the defense intelligence agencies, personal freedoms and also at risk. The question is achieving and maintaining a balance in deciding how to best preserve inalienable constitutional rights against possible incursions by technologists, whether inadvertent or intentional, as our Nation deals with the very real threats both at home and abroad.

Technology gives us wonderful tools, but it can also be a fertile ground for abuse of privacy. We have a responsibility as Congress to exercise oversight in U.S. intelligence agencies, and that can be difficult since much cannot be debated in open forums with any degree of specificity without bringing great harm to the nation. That is why we have the expertise of standing committees. Not only do they understand these issues, it saves time by allocating the proper amount of time to the discussion of these issues in advance. And from the testimony received in the Rules Committee, I believe that Chairman ROGERS and Ranking Member RUPTERSBERGER have demonstrated a strong bipartisan commitment on this issue.

Provisions of this bill are aimed at bolstering personal and individual privacy. Passage of H.R. 4681, when you combine it with the passage last week of the U.S. FREEDOM Act, is a good step for ensuring our U.S. intelligence capability as well as congressional oversight on these issues.

It is a good bill. It is a fair rule. I urge its adoption.

Ms. JACKSON LEE. Mr. Speaker, I rise to speak on the Rule for H.R. 4681, the “Intelligence Authorization Act for Fiscal Years 2014,” and H.R. 4745, the “Transportation, Housing and Urban Development and Related Agencies Appropriations Act of 2014.”

H.R. 4681 is a bill authorizing appropriations for our nation’s intelligence agencies for Fiscal Year 2014 through Fiscal Year 2015. The bill provides funding for our contact with intelligence and intelligence-related activities.

H.R. 4745 makes appropriations for the Departments of Transportation, and Housing and Urban Development, and related agencies for the fiscal year ending September 30, 2015.

Our nation is long past due for a Transportation and Housing and Urban Development Appropriations bill. This bill is about jobs—jobs—jobs.

Unfortunately, H.R. 4745, $17.1 billion in discretionary appropriations for the Department of Transportation for fiscal year 2015, is $727.3 million below the funding for fiscal year 2014.

Included in the legislation is $15.7 billion in total budgetary resources for the Federal Aviation Administration (FAA), which is $7.3 million below the fiscal year 2014 enacted level and $446 million above the request. This will provide full funding for all air traffic control personnel, including 14,800 air traffic controllers, 7,300 safety inspectors, and operational support personnel.

The bill also fully funds the FAA’s Next Generation Air Transportation Systems (NextGen) at $852.4 million, and funds Contract Towers at $140 million.

These investments will help ease future congestion and help reduce delays for travelers in U.S. airspace.

The Bush Intercontinental Airport and William P. Hobby Airport will benefit from funding provided under this bill: nearly 40 million passengers traveled through Bush Intercontinental Airport (IAH) and an additional 10 million traveled through William P. Hobby (HOU); more than 650 daily departures occur at IAH; IAH is the 11th busiest airport in the U.S. for total passenger traffic; IAH has 12 all-cargo airlines handles more than 19,205 metric tons of cargo in 2012.

The funds being sent back to states will repair critical transportation infrastructure that is vital to local, state and the national economy. Further the bill provides for funding for our Nation’s housing and urban development programs that serve our Nation’s elderly, young, disabled, and veterans.

The legislation includes a total of $40.3 billion for the Department of Housing and Urban Development, a decrease of $769 million below the fiscal year 2014 enacted level and $2 billion below the Administration’s request.

The bill does not contain funding for any new, unauthorized “sustainable,” “livable,” or “green” community development programs.

Affordable safe housing is vital to the well-being of elderly, low-wage workers, the unemployed, under-employed, disabled persons and our Nation’s veterans.

In 2012, Texas ranked second among the 50 states among states with workers earning at or below the federal minimum wage. According to the U.S. Bureau of Labor Statistics, of the 6.1 million workers paid hourly rates in Texas in 2012, 282,000 earned exactly the prevailing federal minimum wage of $7.25 per hour, while 170,000 earned less.

In the State of Texas the percentage of persons living in poverty makes the funds provided for housing and mass transit systems including light rail critical: 34% of children live in poverty; 21% of adults (19–64) live in poverty; and 17% of elderly live in poverty.

The funds provided will make it possible for low wage workers to have affordable options for travel as well as support access to affordable housing.

Included in the bill is $26.3 billion for Public and Indian Housing. This is an increase of $6.2 million above the fiscal year 2014 enacted level and $1.2 billion below the requested level. This funding will provide for continued assistance to all families and individuals currently served by this program. The bill also fully funds the President’s request for veterans’ housing vouchers at $75 million.
May 30, 2014

CONGRESSIONAL RECORD—HOUSE

H5035

In the Committee of the Whole

Accordingly, the House resolved itself into the Committee of the Whole House on the state of the Union for the consideration of the bill (H.R. 4681) to authorize appropriations for fiscal years 2014 and 2015 for intelligence and intelligence community management accounts, and for other purposes, with Mr. Poe of Texas in the chair.

The Clerk read the title of the bill.

The CHAIR. Pursuant to the rule, the bill is considered read the first time.

The gentleman from Michigan (Mr. Rogers) and the gentleman from Maryland (Mr. Ruppersberger) each will control 30 minutes.

The Chair recognizes the gentleman from Michigan, Mr. Rogers of Michigan. Mr. Chairman, permit me, I yield myself such time as I might consume.

The Intelligence Authorization Act is the annual blueprint for the work of the intelligence community and America's military intelligence efforts. The bill sets the priorities for our critical intelligence efforts and the legal framework of guidance and oversight for those efforts.

Since the ranking member and I have assumed the leadership of this committee, we passed three intelligence authorization bills in a bipartisan fashion and hope to continue the tradition and trend with H.R. 4681. Passing a yearly intelligence authorization bill is the primary method by which Congress exercises its budgetary and oversight authority over the intelligence community.

As most of the intelligence budget involves highly classified programs, the bulk of this committee's recommendations, which are found in the classified annex to the bill which have been available for Members to review.

Among other initiatives, the bill increases funding to address insider threats and improve personnel security programs.

At an unclassified level, I can report that the annex for fiscal year 2014 authorizes funding that is slightly below the President's budget request level. Its funding levels are in line with the levels appropriated by the enacted appropriation for the National Intelligence Program and with the National Defense Authorization Act for the Military Intelligence Program.

For fiscal year 2015, the bill increases the President's budget request by less than 1 percent and stays within the Bipartisan Budget Act funding caps. The modest increase reflects the committee's concern that the President's request does not properly fund a number of important initiatives and leaves several unacceptable shortfalls.

The legislative provisions that the committee and Congress consider each year are comprised of changes to statute that better enable the community to conduct its important mission and strengthen oversight mechanisms where needed.

Mr. Chairman, we find ourselves in a very interesting time in history. Al-Qaeda and its dangerous affiliates, safe havens have emerged in Syria, parts of Libya, Yemen, Somalia, and the tribal areas of Pakistan. Al-Qaeda is also regaining a foothold in northeast Afghanistan just as the President announced a complete withdrawal of U.S. forces, and the counterterrorism capability that comes with it by the end of 2016.

Uneven leadership in recent years has emboldened adversaries like Russia and China, who are increasing their military and intelligence spending and working to change the international order, as we speak, to the detriment of U.S. interests. Russia occupies 20 percent of the nation of Georgia, invaded and occupied Crimea, threatens invasions, and is bullying its neighbors and expanding claims in the South and East China Seas through which 40 percent of world travel trades.

At the same time, North Korea continues its belligerent behavior, and Iran is maneuvering to preserve its capability to develop a nuclear weapon. A nuclear Iran would threaten Israel with annihilation and send the Middle East into a dangerous nuclear arms race.

We rightly demand that our intelligence agencies provide policymakers with the best and most timely information possible on all these and other threats. We ask them to track terrorists wherever they train, plan, fundraise. We ask them to stop devastating cyber attacks that are stealing American prosperity and American jobs. We ask them to track nuclear and missile threats. And we demand that they get it right every time. Now we are programming it with fewer resources and with what can be described as confusing direction from our Commander in Chief.

The dedication of men and women of the intelligence community who volunteer to serve in some of the most difficult places on Earth are some of the finest patriots I have ever had the privilege to meet. And within budget constraints and unclear policy guidance from the White House, this bill ensures that they have resources and authority to accomplish our Nation and our people safe and accomplish their mission.

As this is the last authorization act I will advance as chairman of the Intelligence Committee, I want to publicly thank my ranking member, my friend, DUTCH RUPPERSBERGER. I can't tell what you a privilege it has been to work with a partner like DUTCH in working through some very difficult issues at a very difficult time in our Nation's history.

National security policy should not be partisan, and we have done everything in our power to ensure that this committee at least takes as non-partisan a view of national security as is humanly possible. It is an honor to work with someone who is also interested in governing and in making progress on an issue so important to our Nation's future.

I would like to thank and urge Member support of H.R. 4681, and I reserve the balance of my time.

Mr. RUPPERSBERGER. Mr. Chair, I yield myself such time as I may consume.

Chairman ROGERS, I thank you for your comments. I also have the same comments for you.

When we took the leadership of this committee, we knew that the stakes were so high and that we had to work together on behalf of the people of the United States of America. We came together with Republicans, Democrats, liberals, conservatives, moderates, all realizing that we had to come together. Because of your leadership, because of Mr. Rogers, we have been able to pass FISA, and hopefully we will be able to pass these bills today.

We are going to miss you, but you will always be there as my friend, and I will always respect you as a great American who cares about the United States. Thank you.

Now, we need to pass this Intelligence Authorization Act for Fiscal Years 2014 and 2015 to ensure rigorous oversight and accountability over all U.S. intelligence agencies and all U.S. intelligence activities. This is so important.

We cannot go back to the days when we give the intelligence agencies a blank check to spend as they see fit. We must have oversight. Remember, Congress specifically amended the National Security Act of 1947 to replace blanket intelligence appropriations with specific authorization.

Why did we do this? To ensure that our intelligence agencies spend money on programs of which Congress is informed and approves. So today we need to make sure we maintain this means of critical oversight by passing the bill.

The Intelligence Authorization Act for 2014 and 2015 is in four parts: the unclassified legislative text; the unclassified report; the classified annex, which explains our intent for the classified aspects of the bill; and the classified schedule of authorizations for both fiscal years. We have been encouraging all Members to review all parts of the bill, and I am pleased to say that they have come to the Intelligence Committee's SCIF, classified spaces, to do so.

The budget for fiscal year 2014 is slightly below the President's budget request, while the budget for fiscal year 2015 is less than 1 percent above the President's budget request.

We both, we made cuts to certain areas and added money in other areas in a responsible, well thought-out way, and a fiscally prudent way.
Since Chairman Rogers and I assumed leadership of the committee, we reduced the Intelligence Committee’s budget by 20 percent, but this year’s bill acknowledges the need to right the ship after the storm of sequestration.

The bill also mentions some specifics. The bill continues to emphasize the value of our satellites; scales back the intelligence community’s use of contractors; pushes for further improvements in the continuous evaluation of insider threats; provides critical forward-looking funding for Navy airborne intelligence surveillance reconnaissance to maintain military intelligence capabilities during the transition to newer, more capable aircraft; and works with the recalcitrant and retention of the best and the brightest for our cyber workforce, particularly within the FBI. Our younger generation, we must educate them and have them stick in this area.

We have spent months poring over this bill and its specific authorizations in great detail—in our committee spaces, at the agencies, and in the remotest corners of the Earth where our intelligence professionals operate—and then I can say this is a very good bill, and I am proud to support it.

Many of the amendments on the floor today also promise to make a great bill even better.

For the sake of keeping the country and its allies safe, and for the sake of rigorously overseeing even the most classified intelligence programs, I urge my colleagues to pass this bill today.

Mr. Rogers of Michigan. Mr. Speaker, I yield 3 minutes to the gentleman from North Carolina (Mr. Pittenger).

Mr. Pittenger. Mr. Chairman, I thank Chairman Rogers for this opportunity to speak. I just really want to commend you for your exceptional leadership as a Member of this body and for your service on behalf of the security of our Nation.

Over the past year, it has really been a privilege to get to know you and work with you on several initiatives. I am just grateful for the way that you handle the people’s business, look forward to working with you more, and also congratulate you on your future endeavors.

The legislation before us today provides the intelligence community the authorization needed to protect and defend our states and support critical national security programs, such as those protecting Americans against terrorism and cyber attacks.

As Members of Congress, we took an oath to the Constitution, which sets forth our duty to provide for the defense of the United States.

Passing the yearly Intelligence Authorization Act is a critical component of living up to our constitutional obligations, ensuring America’s intelligence agencies have the resources necessary to keep Americans safe.

Passing the intelligence authorization is also vital to our important responsibility of providing oversight to the current intelligence community. This legislation ensures Congress, and not the executive branch, is controlling how taxpaying money is being spent on intelligence activities and doing so in the most efficient and effective way possible.

We must remember that we have not defeated the threat of terrorism. The terrorists we face today are not a backyard gang; they are sophisticated and have access to the most modern of technologies.

Over the last 2 years, we have seen the number of worldwide deaths from terrorism attacks double from 10,000 in 2012 to 20,00 in 2013.

These threats, and we in America are able to sleep soundly at night is a credit to the men and women who serve our country selflessly. We must continue to provide these brave men and women every tool possible as they continue to provide for our safety.

That is why I encourage all my colleagues to join me in supporting this legislation.

Mr. Ruppersberger. Mr. Chairman, I yield 2 minutes to the gentlewoman from Illinois, Jan Schakowsky, as a member of our committee, who has been very thoughtful and has allowed us to do the things that we needed to do.

Ms. Schakowsky. Mr. Chairman, I thank the ranking member for yielding.

I want to begin by saying that I really appreciate the way in which our committee operates and has come to present this authorization bill to the floor, but I do want to raise some concerns.

One of the most controversial issues surrounding our national security is the use of the drone program. A number of us tried to introduce some amendments that would be considered on the floor of the House so that we, along with the American people, could have a conversation about that. These amendments were not made in order. And I want to express what my amendment would have done.

It would have limited elements of the intelligence community from engaging in so-called signature strikes. That is, lethal strikes in which the target is not specifically identified but whose so-called pattern of life fits the profile, or signature, of a terrorist.

In these situations, we don’t know the identity of the target. Instead, we draw conclusions from surveillance about whether someone is affiliated with a terrorist organization, or engaged in terrorist conduct. The stakes are high, and inevitably mistakes will be made. There are reports from human rights organizations in past years that we have already made several grave errors, and innocent lives have been lost as a result.

We need to recognize that each mistake we make in these situations killing innocent people spawns more numerous and more determined adversaries, undermining our mission there in the first place.

How we are perceived abroad matters. Even if some of the strikes reported as mistakes are not mistaken, the fact is that the rest of the world perceives our activities as killing innocent civilians and painting all adult male Muslims in these regions as our enemies.

I understand the targeted use, but I think that we cannot kill our way out of this problem and our way to victory.

Mr. Rogers of Michigan. Mr. Chairman, I yield myself such time as I may consume.

Mr. Chairman, I just want to thank the gentlelady from Illinois for her good work and also congratulate her on her future leadership of the committee, who has been very thoughtful and certainly well discussed and well overseen in the spaces where appropriate, and under the appropriate form and function. I think that because there is no aspect of that counterterrorism strategy that isn’t reviewed both in policy leading up to the daily and monthly counterstrategy meetings that happen in the appropriate agencies and departments, I think that we need to continue to work on the oversight of these particular programs.

But I do think it is important to understand something: that all of the focus seems to be on the type of a weapon system that we have used or decided to use or may be using to fight what is a large and growing threat to the United States of America.

I think it was interesting that in the Boko Haram case of the 300 girls, it caught the world’s attention, that you could have a group that was so diabolical that they would kidnap 300 girls and sell them into slavery or force them into marriage and do other unspeakable things. Yes, that is right, that is who these groups are. This is the same group that has threatened the United States of America with terrorist attacks. It is an al Qaeda affiliate. We have watched them cut off the heads of other human beings for the purposes of intimidation, we have watched them cut off other women or have watched them shoot little girls who got on buses to try to go and get an education.

We need to understand what threat faces the United States of America. Because our intelligence services have been so good and so aggressive, we haven’t had an attack here in the same 9/11 fashion—and some of that, by the way, was just sheer luck preparing for the opportunity to catch them.

We need to step back and make sure we are understanding what we are trying to accomplish here and how we try to accomplish it. I think disparaging the very men and women who I know
Mr. ROGERS. Mr. Chairman, I thank you for the work that you have done for the Nation and, certainly, for the commitment that you have made to the very important business of this committee.

Mr. ROGERS, I thank you for the work that you have done for the Nation and, certainly, for the commitment that you have made to the very important business of this committee.

Mr. RUPPERSBERGER, Mr. Chairman, I yield 2 minutes to the gentleman from Texas, SHEILA JACKSON LEE, a great Member of Congress.

Ms. JACKSON LEE. Let me thank the ranking member for yielding and, as well, the chairperson, and let me collectively add my appreciation for the two leaders of this committee.

They have committed themselves, without question, to the security of this Nation. I thank them for their collaboration.

Mr. Rogers, I thank you for the work that you have done for the Nation and, certainly, for the commitment that you have made to the very important business of this committee.

Mr. RUPPERSBERGER, let me thank you for your friendship as well and for the continued collaboration on an issue of great concern to me, but I will speak generally about this legislation and will, again, acknowledge some of the changes that you have looked at and considered and have even included in this legislation as it comes forward.

Mr. Chairman, I agree that detecting and disrupting and preventing a national security crisis is of paramount responsibility for this committee and many others, including the committee that I serve on, the Committee on Homeland Security. For that reason, I have interfaced with this committee on a number of issues.

I am very glad to note, in particular, that the issue of dealing with the expansive use that has been used, which I will talk about in the en bloc amendment, is clearly something that we should have considered, and in this bill, it did.

It got its hand around the enormous use of outside contractors in the intelligence business, and it emphasized recruitment and training. That is positive, and I am pleased.

I yield the bill.

Ms. JACKSON LEE. Let me thank the two leaders of this committee.

Now, particularly with this legislation, I also want to appreciate the collaboration between the Committee and this committee on the USA FREEDOM Act, and I want to say to America that we have corralled the megadata collection. We have done it in a bipartisan manner, and we will do more and do better.

So it is with appreciation for this legislation and in thanking the committee for working with my staff on
my amendment that I ask my colleagues to support this legislation.

Mr. Chair, I rise to speak on H.R. 4681, the Intelligence Authorization Act for fiscal year 2014.

I want to thank the Permanent Select Committee on Intelligence for including my amendment in an en bloc.

My amendment to H.R. 4681 is simple and will be an important addition to the legislation, which I believe can be supported by every member of this Committee.

My amendment seeks greater transparency to Congress on the people who the Nation relies upon to perform certain types of work required of the Intelligence Community.

The Jackson Lee amendment requires the Director of the Office of National Intelligence to conduct an assessment of the reliance of intelligence activities on contractors to support Government objectives, including an assessment of contractors performing intelligence activities, which would include intelligence analysis.

The amendment would seek information on the skills necessary to perform intelligence-related work and whether Federal employees had these skills. The amendment would also seek statistics on contractors preforming intelligence-related work for agencies under the purview of the Director of National Intelligence.

Something is very wrong when the process for screening and vetting government contractors does not identify someone who would have access to—as well as the ability to collect and remove sensitive information from government computers and publicly disclose that information.

If each person working in an intelligence role within the government decided to act on their own thoughts for their own purposes on whether they would or would not keep their oath to defend and protect our Nation’s secrets then there would be chaos.

Our Nation suffers harm in ways we can see, as well as ways that we cannot see when unauthorized disclosures regarding intelligence resources occur.

It harms our ability to work with other nations who rely on our ability to keep secret the information they share with our Nation’s intelligence agencies.

If our global assets and allies cease to trust our ability to keep their work with our intelligence, national defense or diplomatic agencies secret then they will not cooperate with us in our efforts to defend our Nation and our interest around the world.

Reckless disclosures make us vulnerable to our Nation’s enemies who could make changes regarding how we utilize this information because the disclosure of national secrets reveals means and methods.

The world is a dangerous place—we have seen within the last 18 months—a bombing during the Boston Marathon, the rise in sectarian violence in Syria that included incidents involving the use of nerve gas; and Boko Haram which kidnapped nearly 300 girls from their school in northern Nigeria.

According to the United States Department of State Country Report on Terrorism 2013, published in April of this year indicates that there are 53 Foreign Terrorist Organizations (FTOs).

Designation of FTOs is important to our Nation’s fight against terrorism and is effective in cutting off support for those groups so designated.

In 2013, Ansar al-Dine, Boko Haram, and Jama’atu Ansarul Muslimina Bi Biladis-Sudan were added to the list of FTOs.

FTOs are legally defined under Section 219 of the National Security Act of 1947 which states the group must be: a foreign organization; engage in terrorist activity or retain the capacity and intent to engage in terrorist activity or terrorism; and participating in terrorist activity or terrorism that threatens the security of the United States or its citizens.

The United States National Security encompasses national defense, foreign relations, or economic interest.

The unauthorized intelligence disclosures last year implicated U.S. national security.

The intelligence breach came as a result of a government contractor making public sensitive information is still resonating both internationally and within the United States, where an important debate on privacy and civil liberties is still ongoing.

But also around the world the consequences of the unauthorized release of international activity by intelligence agencies is still playing out.

The timing of the release of information on the non-U.S. activity of our intelligence agencies caused tremendous tension in our relations with allies when the United States was working to form a global response to the use of chemical weapons against civilians in Syria.

In addition to frustrating our efforts to form a strong global response to the use of chemical weapons in Syria it also caused economic harm to U.S. companies internationally.

Congress is not able to fully investigate the circumstances that resulted in last year’s intelligence breach because the person with many of the answers to questions many of us have is now living in Russia.

However, we can look prospectively on how the work of the Intelligence Community under the direction of the Office of the Director of National Intelligence should fill positions that require security clearances.

The unauthorized intelligence disclosures have access to—as well as the ability to collect and remove sensitive information from government computers and publicly disclose that information.

The Office of the Director of National Intelligence 2013 Report on Security Clearance Determinations states that by October 1, 2013 the Nation had 3,738,026 Federal agency employees working for the: Office of the Director of National Intelligence Scattered Castles; Department of Defense; Joint Personnel Adjudication System; Office of Personnel Management; and Central Verification System (CVS).

Congress must have the ability to make decisions regarding how intelligence agencies fill positions that require security clearances because it has implications for the appropriations process.

The Information Security Oversight Office of the National Archives 2012 Report to the President focuses on the classification practices of intelligence agencies.

The report addresses the power of “original classification authorities” also called “original classifiers,” which are individuals designated with Top Secret original classification authority to classify information.

Only original classifiers are authorized to determine what information, if disclosed without authorization, would be expected to cause damage to national security.

The original classification authority process complements all other aspects of the security classification system. In 2004, the total number of original classifications was 351,150 and in 2012 the number was 74,477.

The cost of government security classification in 2005 was $7.66 billion and in 2011 the total was $11.36 billion.

The amount expended in 2011 included: 5.65 billion for protection maintenance; 1.53 billion for security management oversight and planning; 502.51 million for professional education, training and awareness; 352.4 million for protection management; and 52.76 million for declassification.

These costs cited are not all encompassing, but were generated by 41 executive branch agencies including the Department of Defense.

The funds expended do not include activity by the Central Intelligence Agency, the Defense Intelligence Agency, Office of the Director for National Intelligence, the National Geospatial-Intelligence Agency, the National Reconnaissance Office, and the National Security Agency.

The focus on training is critical in the work of the Intelligence Community and it is important that this is a high priority for the agencies represented in the National Archive report.
The work by the Intelligence Community to address classification in an evenhanded way can help create and maintain a firm basis for classification of information that is sustainable and can go a long way in addressing questions regarding what secrets are critical to our nation’s national security and what the public has a right to know.

I thank my colleagues on the Intelligence Committee for their hard work in bringing this bill before the full House for consideration. I ask that members of the Congress vote in favor of this bipartisan en bloc amendment to H.R. 4681.

Mr. ROGERS of Michigan. Mr. Chairman, I continue to reserve the balance of my time.

Mr. RUPPERSBERGER. Mr. Chairman, may I inquire as to how much time I have remaining?

The CHAIR. The gentleman from Maryland has 17 minutes remaining.

Mr. ROGERS. I thank the gentleman. I yield 2 minutes to the gentleman from Vermont, Mr. Peter Welch, my good friend and a great Member of Congress.

Mr. Welch. I thank the gentleman. I thank you for your good work.

Mr. ROGERS. I thank you for your good work, and we are going to miss you. Your leadership on the Intel Committee has been of great benefit to this institution. Thank you.

Mr. Welch. I have been working with a number of my colleagues, particularly with Cynthia Lummis of Wyoming, on a question that we think is quite important to the security status of our country, and that is more transparency on behalf of the American people.

This is debated because, by definition, if it is intelligence activity, it is “secret,” but on the other hand, the whole point of having transparency in budgets is to be able to assign the rules of accountability apply across the board. We have 16 different intelligence-gathering agencies, and in all cases, the topline budget is absolutely secret.

The 9/11 Commission that was a bipartisan effort of respected national security credentialed people—Lee Hamilton and the Governor of New Jersey, Governor Keane—recommended that this topline number in the intelligence agency budgets be transparent.

Why? So that there is a basis for taxpayers and for all of us to start to evaluate whether we are getting our money’s worth, whether there is duplication in efforts, whether one agency is stumbling into another, whether there is coordination, whether there is cooperation.

The same reasons that we would have the food stamp budget subject to rigid review and accountability applies as well to our security. In fact, it is enormously important that this country be getting its money’s worth.

The principle of transparency would not in any way compromise, in the view of many respected intelligence leaders like Lee Hamilton, the intelligence agencies and all U.S. intelligence activities, I urge my colleagues to vote for this important, bipartisan bill. I also urge my colleagues to support this bill for the sake of our brave intelligence professionals, who, like our military, work day and night, often in the most austere of places, to keep us safe and our allies safe; and for the sake of all of us—not just in America, but around the world—who benefit from the work of our intelligence agencies. I urge you to vote for this bill. It is a solid bill that we should be proud to support.

Finally, once again, Mr. Chairman, let me thank you for your leadership, our relationship, and your commitment to the people of the United States of America. You served in the military, and you served in the FBI. We are going to miss you.

Thank you also to every member on the Intelligence Committee. We have had many debates, many hard negotiations, and many tough struggles, but at all times, whether or not one member or another agreed or disagreed, we respected the fact that another member had another point of view, and then we resolved those issues.

Each of us has worked even harder to find common ground on behalf of the American people to protect us from terrorist attacks and other issues that are out there that relate to national security.

I yield back the balance of my time. Mr. ROGERS of Michigan. Mr. Chairman, I yield myself the balance of my time.

I thank the ranking member for his work.

Let the American public understand what happens. There are so many assumptions thrown at us about this, so many that serve on the Intelligence and on other committees who must do their work in secret, and certainly, the staff fights through and works through all of these difficult issues.

That despite what you might read in the newspaper, it might not be on the front page of the newspaper. We call that “disaster day” in the business of trying to protect American secrets.

When the ranking member and I first took over the committee, we re-instituted all of the regular oversight patterns: counterintelligence matters, covert action matters, regular counterterrorism strategy updates, and reviews.

Again, every piece of that strategy that is implemented is reviewed by the committee, and it is certainly read and reviewed by me, personally, and I know, by others on the committee as well.

There is a tremendous amount of effort and energy applied to trying to get this right, to making sure that two things happen—one, that they are comporting with the law. They want to do it, they want Congress’ support for what they are doing, and they want the American people’s support for what they are doing—because it is so difficult and so hard to come to the right conclusions in a very murky and dangerous world—so that oversight does happen. It happens regularly.

I want to thank all of the members of both parties for rigorous debate behind those closed doors. There is no loveliest when those doors close and a “let’s just do what we have to do to get to tomorrow.”

The debates are real and vigorous, and we have different philosophies on how we move forward on some of these intelligence matters and collection matters and on how we balance privacy and civil liberties and security. All of that happens.

Sometimes, we find members who just don’t agree, but what we do in that space is understand and try to get and find common ground on a support the resources and all of the policies and all of the authorities our intelligence services need to be impactful to save the
United States and to, yes, maybe even save 300 girls or to, yes, maybe even allow for girls in a place like Afghan- 
istan to get an education. That part needs to be right, too.

Nuclear proliferation—we have a cyber in the Middle East and the largest national security threat to this coun-
try that we are not prepared to handle, and there are a lot of sidebar discus-
sions that have nothing to do with the fact that nation-states are stealing our in-
tellectual property—nation-states like China.

You have, according to public re-
ports, countries like Iran that are prob-
ing financial institutions right here in the United States and are try-
ing to do destructive attacks.

According to public reports, North Korea even attacked a bank in South 
Korea some months ago. You see China rising up in its influence in the South 
and East China Seas. You see potential conflict between Vietnam, Japan, and 
China.

These are serious, serious matters. 
Because they are so far away, I think 
sometimes we forget, and we come to talk about things that are important— 
in how we move forward in the intel-
ligence business and how we empower 
them to do the work of the United States.

At the same time, this recent year of. 
I think, ascension to the men and 
women who serve in these capacities is 
disheartening. This isn’t a new thing.

George Washington used the intel-
ligence business to try to win the war 
against the British.

Ben Franklin is credited with the 
first covert action programs by trying to 
influence British and Tory opinion 
during the first years of the war. John 
Jay created the first counterintel-
ligence unit to try to fight back 
against what the British were doing in 
spying against the Americans.

Jefferson Madison had secret 
funds that they took, by the way, 
which we would no longer approve or 
support today—secret funds—in order 
to do covert action-type activities in the 
earliest days of the founding of our Nation.

We need to stop for a minute and 
think about what is at stake. I think 
the future and safety and security of the 
United States is at stake, and we have 
somehow, over the last year, de-
cided our intelligence services are the 
problem.

No, I have bad news. Actually, I have 
good news: they are part of the solu-
tion. If you don’t want troops engaged 
in the withdrawal of certain diplomatic 
and economic trade arrangements 
around the world, then you want the 
best intelligence services that you can possibly get. Here is the good news: we 
have them. We just need to stand be-
hind them.

When they come home from doing 
big things, when they lose their col-
leagues—and they do—they are not 
looking for a ticker tape parade in New 
York City. They know that is not going 
to happen.

What they do want to understand is 
that, when they turn around, 
the American population and the American 
citizens are standing with them. Even 
though Americans can’t give them the “atta-boy,” we can. Those of us who do 
this work, we can.

So I would tell them, on this floor 
today, on behalf of a grateful Nation, 
thank you for your service. Stop read-
ing the newspaper. Keep doing your 
job. It will mean the difference of lives 
saved around the world.

We have so many challenges, and I 
only say this—and I wasn’t planning to 
say this, Mr. Chairman—that someone 
came on this floor and said: I don’t 
think the intelligence people, but I don’t like their culture.

These are people who are willing to 
risk their lives for that flag that stands in the well of this House. They 
stand up for the act of intelligence they stuck up their hand to 
support.

Is that the culture we don’t like and 
appreciate anymore in America?

There have been some bumps in the road, but we applaud these people. We ought to sing 
their praises.

We ought to thank them every single 
day that they are away from their fam-
ilies, in dangerous places, and risking their lives to collect that one piece of 
information that maybe saves the girls of Boko Haram or maybe saves the 
girls who get on their bus today in the United States of America.

I hope we shake ourselves out of this 
notion that we can just continue to beat them and disparage them and call 
them everything but great patriots and 
expect them to get up every day and do 
the job that they need to do to protect this country.

This bill, I think, actually does that. 
We give them clear guidance. We invest 
in technology that we need to make 
sure that we keep up with our adver-
saries around the world who, by the 
way, are trying to beat us and take ad-
vantage of us—places like space, places 
like cyber, places like HUMINT intel-
ligence, and what they believe is a per-
cieved weakness to deal with a rising 
China.

This is an important bill because it is 
bipartisan. A lot of these issues that 
are talked about have been fought in 
the bowels of this House, basically.

And we worked through it and we have 
come to an agreement that this is the 
right direction, in a bipartisan way, 
that will serve to protect the United States.

So, Mr. Chair, I urge all Members to 
strongly support this bill. Give them 
the tools, give Congress the oversight, 
and give America the ability to sleep 
well at night, knowing that very brave 
men and women will do the work that 
so many would not be interested in 
doing.

With that, Mr. Chairman, I yield 
back the balance of my time.

Mr. MCCAUl. Mr. Chair, I rise today in sup-
pport of H.R. 4681, the “Intelligence Authoriza-
tion Act for Fiscal Years 2014 and 2015.”

As Chairman of the Committee on Home-
land Security, I understand the importance of this legislation. H.R. 4681 en-
highs the national security of the United States and is a vital tool for Congressional oversight of the ac-
tivities of the Intelligence Community. It is crit-
ical that our intelligence agencies have all of 
the resources and authorities they need to ac-
complish the important responsibility of keep-
ing Americans safe. I commend Chairman ROGERS and Ranking Member RUPPERS-
BERGER for their tireless work on these issues and the exhaustive process of drafting a bipar-
sisan authorization.

H.R. 4681 authorizes Federal inte-
ligence, intelligence-related, and 
information sharing activities, including those of the Department of 
Homeland Security’s Office of Intelligence and 
Analysis (I&A). I&A is an element of the De-
partment of Homeland Security (DHS) as well 
and my committee has jurisdiction over this role. I&A supports and collabor-
ates with State and local partners through the 
National Network of Fusion Centers, and pro-
vides analytic support to the DHS compo-
nents.

Consistent with our jurisdiction, the 
Committee on Homeland Security has conducted extensive oversight over these programs and 
missions, to include the July 2013 release of a report on “The National Network of Fusion 
Centers.”

While I support the overall purpose of 
the bill, I am concerned that the effort includes provisions that seek to limit the support I&A 
provides to DHS, its component agencies, and to the 78 fusion centers around the nation. I be-
lieve this risks depriving the Homeland Secu-

rity Enterprise of valuable information and ex-
pertise at a time when we know the threats to 
the homeland persist.

As the bill moves through the process and negotiations begin with the Senate, I will con-
tinue to work to ensure that these issues are 
addressed and that State and local law en-
forcement, and other first responders, receive 
the support they need from the Department of 
Homeland Security.

Mr. CONNOLLY. Mr. Chair, I rise in support 
of my amendment to the Intelligence Author-
ization Act for Fiscal Years 2014 and 2015.

Under Section 307 of this Act, the Chief In-
formation Officer of the Intelligence Com-

munity, along with the respective Chief Infor-
mation Officers of each element that comprise the IC, are required to conduct an inventory of 
every software licenses they used during the year and then assess which, if any, that could be carried out to achieve the greatest 
possible economies of scale and cost-savings in software procurement and usage.
My commonsense amendment simply ensures that when those assessments are carried out, the CIOs will examine leading software license management practices.

By adopting Connolly #12, Congress will ensure that when the IC examines potential actions to enhance software license management, the four leading practices will be included in the analysis.


GAO consulted with software license management experts from the public and private sectors, prior to concluding that Federal agencies are generally not following best practices that could achieve significant cost-savings.

These best practices include increasing the centralization of the management of software licenses; increasing the regular tracking and maintaining of comprehensive inventories of software licenses using automated discovery and inventory tools and metrics; analyzing software license data to inform investment decisions; and providing appropriate personnel with sufficient software licenses management training.

I urge all my colleagues to support my straightforward amendment that will enhance the IC’s ability to spend taxpayer dollars in the most effective and efficient manner possible when procuring and managing software licenses.

The CHAIR. All time for general debate is expired.

Pursuant to the rule, the bill shall be considered for amendment under the 5-minute rule.

In lieu of the amendment in the nature of a substitute recommended by the Permanent Select Committee on Intelligence, printed in the bill, it shall be in order to consider as an original bill for the purpose of amendment under the 5-minute rule an amendment in the nature of a substitute consisting of the text of Rules Committee Print 113-414.

I urge all my colleagues to support my amendment that will enhance the IC’s ability to spend taxpayer dollars in the most effective and efficient manner possible when procuring and managing software licenses.

Title III—General Provisions

Subtitle A—General Matters

Sec. 301. Increase in employee compensation and benefits authorized by law.

Sec. 302. Restriction on conduct of intelligence activities.

Sec. 303. Specific authorization of funding for High Performance Computing/Networking.

Sec. 304. Clarification of exemption from Freedom of Information Act of identities of employees submitting complaints to the Inspector General of the Intelligence Community.

Sec. 305. Functional managers for the intelligence community.

Sec. 306. Annual report on the intelligence community performance by function.

Sec. 307. Software licensing.

Sec. 308. Plans to respond to unauthorized public disclosures of covert actions.

Sec. 309. Auditability.

Sec. 310. Public Interest Declassification Board.

Sec. 311. Official representation items in support of the Coast Guard Attaché Program.

Sec. 312. Declassification review of certain items collected during the mission that killed Osama bin Laden on May 1, 2011.

Sec. 313. Mergers of the Foreign Counterintelligence Program and the General Defense Intelligence Program.

Subtitle B—Reporting

Sec. 321. Annual report on violations of law or rules.

Sec. 322. Submittal to Congress by heads of elements of intelligence community of plans for orderly shutdown in event of absence of appropriation.

Sec. 323. Reports on chemical weapons in Syria.

Sec. 324. Reports to the intelligence community on penetrations of networks and information systems of certain contractors.


Sec. 326. Promoting STEM education to meet the future workforce needs of the intelligence community.

Sec. 327. Assessment of security of domestic oil refineries and related rail transportation infrastructure.

Sec. 328. Repeal or modification of certain reporting requirements.

Title IV—Matters Relating to Elements of the Intelligence Community

Sec. 401. Gifts, devises, and bequests to the Central Intelligence Agency.

Sec. 402. Inspector General of the National Security Agency.

Title V—Security Clearance Reform

Sec. 501. Continual evaluation and sharing of derogatory information regarding personnel with access to classified information.

Sec. 502. Requirements for intelligence communica
tions.

Sec. 503. Technology improvements to security clearance processing.

Sec. 504. Report on reciprocity of security clearances.

Sec. 505. Improving the periodic reinvestigation process.

Sec. 506. Appropriate committees of Congress defined.
SEC. 103. PERSONNEL CEILING ADJUSTMENTS.

(a) AUTHORITY FOR INCREASES.—The Director of National Intelligence may authorize employment of civilian personnel in excess of the number authorized for fiscal year 2014 or 2015 as specified in the classified Schedule of Authorizations referred to in section 102(a) if the Director of National Intelligence determines that such action is necessary to ensure the effective delivery of intelligence functions, except that the number of personnel authorized in excess of the number authorized under such section may not, for any element of the Intelligence Community Management Account as of September 30, 2015, exceed 3 percent of the number of civilian personnel authorized under the Schedule for such element during the fiscal year covered by such Schedule.

(b) AUTHORITY TO REVISE.—The Director of National Intelligence may specify for purposes of this section the Director may designate individuals to serve as manager of intelligence functions established under subsection (a) from among officers and employees of elements of the intelligence community.

(c) DUTIES.—Each manager of an intelligence function established under subsection (a) shall have the duties as follows:

"(1) To act as principal advisor to the Director on the intelligence function;

"(2) To carry out such responsibilities with respect to the intelligence function as the Director may specify for purposes of this section;"}

TITLE III—GENERAL PROVISIONS

Subtitle A—General Matters

SEC. 301. INCREASE IN EMPLOYEE COMPENSATION AND BENEFITS AUTHORIZED BY SEC. 102A.

There is authorized to be appropriated for the Intelligence Community Retirement and Disability Fund $514,090,000 for each of fiscal years 2014 and 2015.

SEC. 302. RESTRICTION ON CONDUCT OF INTELLIGENCE ACTIVITIES.

Appropriations authorized by this Act for salary, pay, retirement, and other benefits for Federal employees may be increased by such additional or supplementary amounts as may be necessary for increases in such compensation or benefits authorized by law.

SEC. 303. SPECIFIC AUTHORIZATION OF FUNDING FOR HIGH PERFORMANCE COMPUTING CENTER 2.

Funds appropriated for the construction of the High Performance Computing Center 2 (HPCC 2), as described in the table entitled Consolidated Appropriations Act, 2014, and as identified in the classified Schedule of Authorizations referred to in section 102(a) for advanced research and development shall remain available until September 30, 2016.

SEC. 304. CLARIFICATION OF EXEMPTION FROM FREEDOM OF INFORMATION ACT OF IDENTITIES OF EMPLOYEES SUBMITTING COMPLAINTS TO THE INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY.

Section 103H(g)(3)(A) of the National Security Act of 1947 (50 U.S.C. 3033(g)(3)(A)) is amended by striking "undertaken," and inserting "un-".

SEC. 305. FUNCTIONAL MANAGERS FOR THE INTELLIGENCE COMMUNITY.

(a) FUNCTIONAL MANAGERS AUTHORIZED.

Title I of the National Security Act of 1947 (50 U.S.C. 3021 et seq.) is amended by inserting after section 103I the following new section:

"SEC. 103J. FUNCTIONAL MANAGERS FOR THE INTELLIGENCE COMMUNITY.

"(a) FUNCTIONAL MANAGERS AUTHORIZED.—The Director of National Intelligence may establish within the intelligence community one or more positions of manager of an intelligence function. Any position so established may be known as the "Functional Manager" of the intelligence function concerned.

"(b) PERSONNEL.—The Director shall designate individuals to serve as manager of intelligence functions established under subsection (a) from among officers and employees of elements of the intelligence community.

"(c) DUTIES.—Each manager of an intelligence function established under subsection (a) shall have the duties as follows:

"(1) To act as principal advisor to the Director on the intelligence function;

"(2) To carry out such responsibilities with respect to the intelligence function as the Director may specify for purposes of this section;"
(b) TABLE OF CONTENTS AMENDMENT.—The table of contents in the first section of the National Security Act of 1947 is amended by inserting after the item relating to section 506 the following new item:

“Sec. 506J. Annual assessment of intelligence community performance by function.”

SEC. 307. SOFTWARE LICENSING.

(a) IN GENERAL.—Title I of the National Security Act of 1947 (50 U.S.C. 3021 et seq.) is amended by inserting after section 108 the following new section:

“SEC. 109. SOFTWARE LICENSING.

(a) REQUIREMENT FOR INVENTORIES OF SOFTWARE LICENSES.—The Chief Information Officer of each element of the intelligence community, in consultation with the Chief Information Officer of the Intelligence Community, shall biennially—

(1) conduct an inventory of all existing software licenses of such element, including utilized and unutilized licenses; and

(2) assess the actions that could be carried out by the intelligence community to achieve the greatest possible economies of scale and associated cost savings in software procurement and usage;

and submitting reports on such actions to the congressional intelligence committees a copy of each inventory compiled under subsection (a), shall biennially—

(1) compile an inventory of all existing software licenses of the intelligence community, including utilized and unutilized licenses; and

(2) assess the actions that could be carried out by the intelligence community to achieve the greatest possible economies of scale and associated cost savings in software procurement and usage;

(c) REPORTS TO CONGRESS.—The Chief Information Officer of the Intelligence Community shall submit to the congressional intelligence committees a copy of each inventory compiled under subsection (a).

(b) INITIAL INVENTORY.—

(1) INTELLIGENCE COMMUNITY ELEMENTS.—

(A) DATE.—Not later than 120 days after the date of enactment of this Act, the Chief Information Officer of each element of the intelligence community shall complete the initial inventory, assessment, and submission required by paragraph (1) and each assessment required by paragraph (2).

(b) INVENTORIES BY THE CHIEF INFORMATION OFFICER OF THE INTELLIGENCE COMMUNITY.—The Chief Information Officer of the Intelligence Community, based on the inventories and assessments required by subsection (a), shall biennially—

(1) conduct an inventory of all existing software licenses of such element, including utilized and unutilized licenses; and

(2) assess the actions that could be carried out by the intelligence community to achieve the greatest possible economies of scale and associated cost savings in software procurement and usage;

(c) REPORTS TO CONGRESS.—The Chief Information Officer of the Intelligence Community shall submit to the congressional intelligence committees a copy of each inventory compiled under subsection (a), shall biennially—

(1) conduct an inventory of all existing software licenses of such element, including utilized and unutilized licenses; and

(2) assess the actions that could be carried out by the intelligence community to achieve the greatest possible economies of scale and associated cost savings in software procurement and usage;

(c) REPORTS TO CONGRESS.—The Chief Information Officer of the Intelligence Community shall submit to the congressional intelligence committees a copy of each inventory compiled under subsection (a), shall biennially—

(1) conduct an inventory of all existing software licenses of such element, including utilized and unutilized licenses; and

(2) assess the actions that could be carried out by the intelligence community to achieve the greatest possible economies of scale and associated cost savings in software procurement and usage;

(c) REPORTS TO CONGRESS.—The Chief Information Officer of the Intelligence Community shall submit to the congressional intelligence committees a copy of each inventory compiled under subsection (a), shall biennially—

(1) conduct an inventory of all existing software licenses of such element, including utilized and unutilized licenses; and

(2) assess the actions that could be carried out by the intelligence community to achieve the greatest possible economies of scale and associated cost savings in software procurement and usage;

(c) REPORTS TO CONGRESS.—The Chief Information Officer of the Intelligence Community shall submit to the congressional intelligence committees a copy of each inventory compiled under subsection (a), shall biennially—

(1) conduct an inventory of all existing software licenses of such element, including utilized and unutilized licenses; and

(2) assess the actions that could be carried out by the intelligence community to achieve the greatest possible economies of scale and associated cost savings in software procurement and usage;

(c) REPORTS TO CONGRESS.—The Chief Information Officer of the Intelligence Community shall submit to the congressional intelligence committees a copy of each inventory compiled under subsection (a), shall biennially—

(1) conduct an inventory of all existing software licenses of such element, including utilized and unutilized licenses; and

(2) assess the actions that could be carried out by the intelligence community to achieve the greatest possible economies of scale and associated cost savings in software procurement and usage;
(A) In the case of a plan for an element of the intelligence community that is within the Department of Defense, to—

(A) the Committee on Armed Services of the Senate; and

(B) the Committee on Armed Services of the House of Representatives.

(b) HEAD OF AN APPLICABLE AGENCY DEFINED.—In this section, the term "head of an applicable agency" includes the following:

(1) The Director of National Intelligence.

(2) The Director of the Central Intelligence Agency.

(3) Each head of each element of the intelligence community that is within the Department of Defense.

SEC. 323. REPORTS ON CHEMICAL WEAPONS IN SYRIA.

(a) IN GENERAL.—Not later than 30 days after the date of enactment of this Act, the Director of National Intelligence shall submit to Congress a report on the Syrian chemical weapons program.

(b) ELEMENTS.—The report required under subsection (a) shall include the following elements:

(1) A comprehensive assessment of chemical weapons stockpiles, munitions, and facilities.

(2) An analysis of the means of weapons assembly and delivery systems available to Syria.

(3) An examination of the means of weapons storage available to Syria.

(4) An assessment of how the stockpiles, munitions, and facilities were obtained.

(5) A description of key intelligence gaps related to the Syrian chemical weapons program.

(6) An assessment of undeclared chemical weapons stockpiles, munitions, and facilities.

(7) An assessment of the extent to which Syria implemented the chemical weapons program.

(c) DEFINITIONS.—In this section:

(1) "Chemical weapons" means the chemical agents, types of munitions, and location and form of storage, production, and research and development.

(2) "Chemical weapons program" includes all weapons stockpiles, munitions, and facilities.

(3) "Chemical weapons program" includes all weapons stockpiles, munitions, and facilities.

(4) "Chemical weapons program" includes all weapons stockpiles, munitions, and facilities.

(5) "Chemical weapons program" includes all weapons stockpiles, munitions, and facilities.

(d) ISSUANCE OF PROCEDURES AND ESTABLISHMENT OF CRITERIA.—

(1) IN GENERAL.—Not later than 90 days after the date of enactment of this Act, the Director of National Intelligence shall establish procedures to identify and report to an element of the intelligence community to access, retain, and provide for the protection of classified information related to the Syrian chemical weapons program.

(2) APPLICABILITY.—The procedures established pursuant to subsection (a) shall—

(A) include mechanisms for intelligence community personnel to, upon request, obtain access to and to conduct forensic analysis in any chemical weapons program.

(B) provide that a cleared intelligence contractor is only required to provide access to or for an element of the intelligence community in connection with any intelligence community program that was successfully exfiltrated from a cleared intelligence contractor and, if so, what information was exfiltrated.

(C) provide for the reasonable protection of trade secrets, commercial or financial information, and information that can be used to identify a specific person (other than the name of the suspected perpetrator of the penetration).

(e) LIMITATION OF ACCESS TO PERSONAL INFORMATION.—The procedures established pursuant to subsection (a) shall prohibit the dissemination outside the intelligence community of information that was created by or for an element of the intelligence community in connection with any intelligence community program that was successfully exfiltrated from a cleared intelligence contractor and, if so, what information was exfiltrated.

(f) DEFINITIONS.—In this section:

(A) "Cleared intelligence contractor" means a cleared intelligence contractor that is only required to provide access to equipment or information created by or for an element of the intelligence community in connection with any intelligence community program that was successfully exfiltrated from a cleared intelligence contractor.

(B) "Cleared intelligence contractor" means a cleared intelligence contractor that is only required to provide access to equipment or information created by or for an element of the intelligence community in connection with any intelligence community program that was successfully exfiltrated from a cleared intelligence contractor.

(C) "Cleared intelligence contractor" means a cleared intelligence contractor that is only required to provide access to equipment or information created by or for an element of the intelligence community in connection with any intelligence community program that was successfully exfiltrated from a cleared intelligence contractor.

(D) "Cleared intelligence contractor" means a cleared intelligence contractor that is only required to provide access to equipment or information created by or for an element of the intelligence community in connection with any intelligence community program that was successfully exfiltrated from a cleared intelligence contractor.

SEC. 324. REPORTS TO THE INTELLIGENCE COMMUNITY ON PENETRATIONS OF NETWORKS AND INFORMATION SYSTEMS OF CERTAIN CONTRACTORS.

(a) PROCEDURES FOR REPORTING PENETRATIONS.—The Director of National Intelligence shall establish procedures to require each cleared intelligence contractor to report to an element of the intelligence community designated pursuant to subsection (a) of each successful penetration of a network or information system of such contractor that meets the criteria established pursuant to subsection (b) of each such penetration.

(b) NETWORKS AND INFORMATION SYSTEMS SUBJECT TO REPORTING.—The Director of National Intelligence shall, in consultation with the Director of the Central Intelligence Agency, establish procedures for purposes of this section on the networks and information systems of each contractor that meet the criteria established pursuant to subsection (b) of each such penetration.

(c) PROCEDURE REQUIREMENTS.—

(1) RAPID REPORTING.—The procedures established pursuant to subsection (a) shall require each cleared intelligence contractor to rapidly report to an element of the intelligence community designated pursuant to subsection (a) of each successful penetration of the network or information system of such contractor that meet the criteria established pursuant to subsection (b) of each such penetration.

(2) COVERED NETWORK.—The term "covered network" means a network or information system that contains or processes information created by or for an element of the intelligence community.

(3) COVERED NETWORK.—The term "covered network" means a network or information system that contains or processes information created by or for an element of the intelligence community.

(4) COVERED NETWORK.—The term "covered network" means a network or information system that contains or processes information created by or for an element of the intelligence community.

(5) COVERED NETWORK.—The term "covered network" means a network or information system that contains or processes information created by or for an element of the intelligence community.

(6) COVERED NETWORK.—The term "covered network" means a network or information system that contains or processes information created by or for an element of the intelligence community.

(f) SAVINGS CLAUSES.—Nothing in this section shall be construed to alter or limit any otherwise authorized access by government personnel to networks or information systems owned or operated by a contractor that processes or stores government data.

SEC. 325. REPORT ON ELECTRONIC WASTE.

(a) REPORT.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the congressional intelligence committees a report on the extent to which the intelligence community has implemented the recommendations of the Inspector General of the Intelligence Community contained in the report entitled "Study of Intelligence Community Practices on Disposal of Electronic Waste" issued in May 2013. Such report shall include an assessment of the extent to which the policies, standards, and guidelines of the intelligence community prohibited or directed disposal of electronic waste are applicable to covered electronic waste that may contain classified information.

(b) ELECTRONIC WASTE.—The term "electronic waste" includes any obsolete, broken, or irrepairable electronic device, including a television, copier, facsimile machine, tablet, telephone, computer, or any other electronic device, including a scanner, and associated electrical wiring.

SEC. 326. PROMOTING STEM EDUCATION TO MEET THE FUTURE WORKFORCE NEEDS OF THE INTELLIGENCE COMMUNITY.

(a) REPORT.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the Senate and the House of Representatives in each report to the committees and such Subcommittees to perform oversight functions and to the congressional intelligence committees a report describing the anticipated hiring needs of the intelligence community in the fields of science, technology, engineering, and mathematics, including cybersecurity and computer literacy.

(b) ELEVEN YEARS OF EDUCATION TO MEET THE FUTURE WORKFORCE NEEDS OF THE INTELLIGENCE COMMUNITY.

(1) HIGH SCHOOL.—The term "high school" means a school that has the same meaning given such term in section 9101 of the Elementary and Secondary Education Act of 1965 (20 U.S.C. 2001(a)).

(2) COLLEGE.—The term "college" means a school that has the same meaning given such term in section 618(a) of the Elementary and Secondary Education Act of 1965 (20 U.S.C. 7801).

(3) SCHOLARSHIP.—The term "scholarship" means a scholarship or grant given to eligible persons to pursue higher education.

(4) INSTITUTION OF HIGHER EDUCATION.—The term "institution of higher education" means any public or private college or university, including any public or private research university.

(5) POSTSECONDARY.—The term "postsecondary" means any institution of higher education.

(6) SCHOLARSHIP.—The term "scholarship" means a scholarship or grant given to eligible persons to pursue higher education.
SEC. 227. ASSESSMENT OF SECURITY OF DOMESTIC OIL REFINERIES AND RELATED RAIL TRANSPORTATION INFRASTRUCTURE.  
(a) ASSESSMENT.—The Under Secretary of Homeland Security for Intelligence and Analysis shall conduct an intelligence assessment of the security of domestic oil refineries and related rail transportation infrastructure.

(b) SUBMISSION.—Not later than 180 days after the date of the enactment of this Act, the Under Secretary of Homeland Security for Intelligence and Analysis shall submit to the congressional intelligence committees—

(1) the results of the assessment required under subsection (a); and

(2) any recommendations with respect to intelligence sharing or intelligence collection to improve security of domestic oil refineries and related rail transportation infrastructure to protect the communities surrounding such refineries or such infrastructure from potential harm that the Under Secretary considers appropriate.

SEC. 228. REPEAL OR MODIFICATION OF CERTAIN REPORTING REQUIREMENTS.  
(a) REPEAL OF REPORTING REQUIREMENTS.—

(1) THREAT OF ATTACK ON THE UNITED STATES USING WEAPONS OF MASS DESTRUCTION.—Section 114 of the National Security Act of 1947 (50 U.S.C. 3090) is amended by striking subsection (b).


(b) MODIFICATION OF REPORTING REQUIREMENTS.—

(1) INTELLIGENCE ADVISORY COMMITTEES.—Section 1061 of the Intelligence Authorization Act for Fiscal Year 2010 (50 U.S.C. 3309) is amended to read as follows:

“(a) INTELLIGENCE ADVISORY COMMITTEES.—Section 1061 of the Intelligence Authorization Act for Fiscal Year 2010 (50 U.S.C. 3309) is amended—

(1) in the text preceding subsection (a), by striking “(a)” and inserting “(b)”;

(2) in section 1061 (50 U.S.C. 3309) (A) by amending subsection (a) to read as follows: ‘‘ANNUAL REPORT ON HIRING AND RETENTION OF MINORITY EMPLOYEES.—

(C) by redesignating paragraphs (1) through (5) as paragraphs (1) through (5), respectively; and

(D) in subsection (b) (as redesignated by paragraph (i) by redesignating subparagraphs (A) through (C) as paragraphs (1) through (3), respectively; and

(ii) in paragraph (2) (as so redesignated)—

(I) by redesignating clauses (i) and (ii) as subparagraphs (A) and (B); and

(E) in subsection (d) (as redesignated by subparagraph (C) of this paragraph), by striking “subsection (a)” and inserting “subsection (b)”;

(F) in subsection (e) (as redesignated by paragraph (i) by redesignating subparagraphs (A) through (C) as paragraphs (1) through (3), respectively; and

(ii) by striking “subsection,” and inserting “subsection”;

and

(3) in section 507 (50 U.S.C. 3106)—

(A) in subsection (b), by striking “subsection (c)(1)(A)” and inserting “subsection (c)(1)”;

(i) by striking “(A) Except” and inserting “Except”;

and

(ii) by striking subparagraph (B) and (C) in subsection (d)(1)—

(i) by striking “subsection (a)(1)” and inserting “subsection (a)(2)”;

(ii) by inserting “and” and after “March 1”;

(iii) by striking paragraph (B) and;

and

(iii) by redesignating subparagraph (C) as subparagraph (D).

TITLE IV—MATTERS RELATING TO ELEMENTS OF THE INTELLIGENCE COMMUNITY

SEC. 401. GIFTS, DEVISES, AND BEQUESTS TO THE CENTRAL INTELLIGENCE AGENCY.  
Section 12 of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3024(g)(4)) is amended to read as follows:

“(4) The Director of the Central Intelligence Agency shall, in a timely manner, report to Congress any substantial policy, or practice of the Director believes impedes the ability of the Director to fully and effectively ensure maximum accountability to the intelligence community, or the protection of the national security of the United States.

(5) USG COMMUNITY BUSINESS SYSTEM TRANSFORMATION.—Section 506D(j) of the National Security Act of 1949 (50 U.S.C. 3100(j)) is amended in the matter preceding paragraph (1) by striking “quarterly” and inserting “semiannually”.

(c) CONFORMING AMENDMENTS.—The National Security Act of 1949 (50 U.S.C. 301 et seq.) is amended—

(1) in the table of contents in the first section, by striking the first paragraph of section 114 and inserting the following new item:

“Sec. 114. Annual report on hiring and retention of minority employees.”;

(2) in section 114 (50 U.S.C. 3309) (A) by amending subsection (a) to read as follows: ‘‘ANNUAL REPORT ON HIRING AND RETENTION OF MINORITY EMPLOYEES.—

(A) by redesignating paragraphs (1) through (5) as paragraphs (1) through (5), respectively; and

(B) in paragraph (a), by inserting “Central Intelligence Agency,” after “National Security Agency,” after “Federal Emergency Management Agency,” and;

(B) in paragraph (b), by inserting “National Security Agency,” after “National Aeronautics and Space Administration,”.

(c) DATE OF APPOINTMENT.—Not later than 90 days after the date of the enactment of this Act, the President shall nominate a person for appointment, by and with the advice and consent of the Senate, as Inspector General of the National Security Agency under section 3(a) of the Inspector General Act of 1978 (5 U.S.C. App.), consistent with the amendments made by subsection (a).

(d) TRANSITION RULE.—An individual serving as Inspector General of the National Security Agency on the date of the enactment of this Act pursuant to an appointment made under section 80 of the Inspector General Act of 1978 (5 U.S.C. App.)—

(1) may continue so serving until the President makes an appointment under section 3(a) of such Act with respect to the National Security Agency consistent with the amendments made by subsection (a); and

(2) shall, while serving under paragraph (1), remain subject to the provisions of section 80 of such Act that, immediately before the date of the enactment of this Act, applied with respect to the Inspector General of the National Security Agency and suffer no reduction in pay.

(d) SPECIAL PROVISIONS CONCERNING THE NATIONAL SECURITY AGENCY.—The Inspector General Act of 1978 (5 U.S.C. App.) is amended by inserting after section 8I the following new section:

“SEC. 8K. SPECIAL PROVISIONS CONCERNING THE NATIONAL SECURITY AGENCY.  
(a) GENERAL COUNSEL TO THE INSPECTOR GENERAL.—

(1) IN GENERAL.—There is a General Counsel to the Inspector General of the National Security Agency, who shall be appointed by the Inspector General of the National Security Agency.

(2) DUTIES.—The General Counsel to the Inspector General of the National Security Agency shall—

“(A) serve as the chief legal officer of the Office of the Inspector General of the National Security Agency; and

(B) provide legal services only to the Inspector General of the National Security Agency;

“(C) prescribe professional rules of ethics and responsibilities for employees and officers of, and contractors to, the National Security Agency;

“(D) perform such functions as the Inspector General may prescribe; and

“(E) serve at the discretion of the Inspector General.

(b) REPORT TO THE OFFICE OF THE GENERAL COUNSEL.—There is an Office of the General Counsel to the Inspector General of the National Security Agency. The Inspector General may appoint to the Office of the General Counsel one or more General Counsel, and such legal counsel as the Inspector General considers appropriate.
(b) TESTIMONY.—

(1) AUTHORITY TO COMPEL.—The Inspector General of the National Security Agency is authorized to require by subpoena the attendance and testimony of any employee or officer of a department, an agency, or an establishment of the Federal Government, or of any element of the intelligence community, a contractor to an element of the intelligence community, an individual employed by, or contracted or detailed to, the National Security Agency as necessary in the performance of duties assigned to the Inspector General by this Act.

(2) REFUSAL TO OBEY.—A subpoena issued under this subsection, in the case of contempt or refusal to obey, shall be enforcible by order of any appropriate United States district court.

(3) NOTIFICATION.—The Inspector General shall notify the Attorney General 7 days before issuing a subpoena under this section.

(4) ENSURING COMPLIANCE.—The Inspector General shall have the power to enforce the effective execution of a subpoena by any means provided by law, including the issuance of a contempt of court order.

(5) PROHIBITIONS ON INVESTIGATIONS FOR NATIONAL SECURITY REASONS.—

(1) EVALUATIONS OF PROHIBITIONS.—Not later than 7 days after the date on which the Inspector General of the National Security Agency receives notice or a statement under section 801(2)(B) of the reasons the Secretary of Defense is prohibiting the Inspector General from initiating, carrying out, or completing any audit or investigation, the Inspector General shall submit to the Permanent Select Committee on Intelligence the Inspector General Committee on Armed Services of the House of Representatives and the Select Committee on Intelligence and the Committee on Armed Services of the Senate an evaluation of such statement.

(2) INCLUSION IN SEMI-ANNUAL REPORT.—The Inspector General shall include in the semiannual report prepared by the Inspector General in accordance with section 3(a), a description of the instances in which the Secretary of Defense prohibited the Inspector General from initiating, carrying out, or completing any audit or investigation during the period covered by such report.

TITLE V—SECURITY CLEARANCE REFORM

SEC. 501. CONTINUOUS EVALUATION AND SHARING OF PERSONNEL INFORMATION REGARDING PERSONNEL WITH ACCESS TO CLASSIFIED INFORMATION.

Section 102A(j) of the National Security Act of 1947 (50 U.S.C. 3024(j)) is amended—

(1) in the heading, by striking “SENSITIVE COMPARTMENTED INFORMATION” and inserting “CLASSIFIED INFORMATION”;

(2) in paragraph (2), by striking “and” and inserting a semicolon;

(3) in paragraph (4), by striking the period at the end and inserting a semicolon;

(4) the standardization of forms used for routine reporting required of cleared personnel (such as travel, foreign contacts, and financial disclosures) and use of continuous monitoring technology for automated collection and reporting of such reportable information to independently obtain and analyze reportable data and events; and

(5) the establishment of an authoritative central repository of personnel security information that is accessible electronically at multiple levels of classification and eliminates baseline bar charts for determining eligibility determinations and reciprocal recognition thereof;

(6) the expansion of the use of technology to improve an individual’s ability to discover the status of a pending security clearance application or reevaluation; and

(7) the use of continuous monitoring in conjunction with mitigating factors to adjudicate guidelines to improve quality and timeliness, and reduce costs, of investigations and reevaluations.

(8) REPORT TO CONGRESS.—Not later than 6 months after the date of the enactment of this Act, the Director of National Intelligence shall submit to the appropriate committees of Congress a report on the analysis required by subsection (a).

SEC. 504. REPORT ON RECIPROCITY OF SECURITY CLEARANCES.

The head of the entity selected pursuant to section 3001(b) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3311(b)) shall submit to the appropriate committees of Congress a report each year through 2017 that describes for the preceding year—

(1) the periods of time required by authorized adjudicative agencies for accepting background investigations and determinations completed by an authorized investigative entity or authorized adjudicative agency;

(2) the total number of cases in which a background investigation or determination completed by an authorized investigative entity or authorized adjudicative agency is accepted by another agency; and

(3) such other information or recommendations as the head of the entity selected pursuant to section 3001(b) considers appropriate.

SEC. 505. IMPROVING THE PERIODIC REINVESTIGATION PROCESS.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, and thereafter every 3 years thereafter until December 31, 2017, the Director of National Intelligence, in consultation with the Secretary of Defense and the Director of the Office of Personnel Management, shall submit to the appropriate committees of Congress a strategic plan for updating the process for periodic reinvestigations consistent with a continuous evaluation program.

(b) CONTENTS.—The plan required by subsection (a) shall include—

(1) an analysis of the costs and benefits associated with conducting periodic reinvestigations; and

(2) the standardization of forms used for routine reporting required of cleared personnel (such as travel, foreign contacts, and financial disclosures) and use of continuous monitoring technology for automated collection and reporting of such reportable information to independently obtain and analyze reportable data and events; and

(3) a determination of how many risk-based and ad hoc periodic reinvestigations are necessary on an annual basis for each component of the Federal Government with employees with security clearances; and

(4) an analysis of the potential benefits of expanding the Government’s use of continuous evaluation tools as a means of improving the efficiency and effectiveness of procedures for confirming the eligibility of personnel for continued access to classified information; and

(5) an analysis of how many personnel with overseas assignments are background reinvestigated or contracted by, or contracted or detailed to, each element of the intelligence community.
and 11 printed in part A of House Report No. 113–465, offered by Mr. McKeeon of California:

AMENDMENT NO. 1 OFFERED BY MR. ROGERS OF MICHIGAN
Page 9, line 17, strike “2014” and insert “2015.”

Page 24, strike lines 1 through 9 and insert the following:

“(b) ELEMENTS.—Each report required under subsection (a) shall, consistent with the need to preserve ongoing criminal investigations, include a description of, and any action taken in response to, any violation of law or executive order (including Executive Order 12333 (50 U.S.C. 3001 note)) relating to intelligence activities committed by personnel of an element of the intelligence community in the course of the employment of such personnel that, during the previous calendar year, was—

(1) determined by the director, head, or general counsel of any element of the intelligence community to have occurred;

(2) referred to the Department of Justice for possible criminal prosecution; or

(3) substantiated by the inspector general of any element of the intelligence community.”.

Page 24, after line 13, insert the following:

“(c) GUIDELINES.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence, in consultation with the head of each element of the intelligence community, shall—

(1) issue guidelines to carry out section 510 of the National Security Act of 1947, as added by subsection (a) of this section; and

(2) submit guidelines to the congressional intelligence committees.

Page 24, line 14, redesignate subsection (c) as subsection (d).

Page 25, before line 20 insert the following:

(e) RULE OF CONSTRUCTION.—Nothing in this section or the amendments made by this section shall be construed to alter any requirement existing on the date of enactment of this Act to submit a report under any provision of law.

Page 43, line 11, strike “the date of the enactment of this Act” and insert “the date of the enactment, reassignment, or removal of the Inspector General of the National Security Agency appointed pursuant to section 803 of the Inspector General Act of 1978 (50 U.S.C. App.) as in effect before the date of the enactment of this Act and serving on such date”.

Page 45, line 9, insert before “the National Security” the following: “the Office of the Inspector General of”. 

AMENDMENT NO. 2 OFFERED BY MR. CONNOLLY OF VIRGINIA
Page 17, line 7, strike “usage; and” and insert “usage, including”—.

Page 17, after line 7, insert the following:

“(A) increasing the centralization of the management by software licenses; and

“(B) increasing the regular tracking and maintaining of comprehensive inventories of software licenses using automated discovery and inventory tools and metrics;

“(C) analyzing software license data to inform investment decisions; and

“(D) providing appropriate personnel with sufficient software licenses management training; and

Page 17, line 23, strike “usage.” and insert “usage, including”—.

Page 17, after line 23, insert the following:

“(A) increasing the centralization of the management of software licenses; and

“(B) increasing the regular tracking and maintaining of comprehensive inventories of software licenses using automated discovery and inventory tools and metrics;
“(1) determine which foreign governments pose a significant counterintelligence threat to the United States; and
“(2) submit to the congressional intelligence committees a list of such foreign governments.
“(e) DEFINITIONS.—In this section:
“(1) COVERED EMPLOYEE.—The term ‘covered employee’ means—
“(A) an employee of an element of the intelligence community with access to sensitive compartmented information occupying a position—
“(i) classified at GS-15 of the General Schedule (chapter 53 of title 5, United States Code); or
“(ii) as a senior civilian officer of the intelligence community (as defined in Intelligence Community Directive No. 610 or any successor directive); and
“(B) a person who during the preceding 12-month period was an officer or employee of the Congress (as defined in section 108(k) of the Federal Bureau of Investigation Act of 1995 (28 U.S.C. App.)) with access to sensitive compartmented information.
“(2) COVERED ENTITY.—The term ‘covered entity’ means—
“(A) any person acting on behalf or under the supervision of a designated foreign government; or
“(B) any entity owned or controlled by a designated foreign government.
“(3) DESIGNATED FOREIGN GOVERNMENT.—
“The term ‘designated foreign government’ means a government that the Director of National Intelligence determines poses a significant counterintelligence threat to the United States.
“(b) EFFECTIVE DATE OF NEGOTIATION PERIOD NOTICE.—The requirement under section 304(a) of the National Security Act of 1947, as added by subsection (a) of this section, shall take effect on the date that is 30 days after the date of the enactment of this Act.
“(c) EFFECTIVE DATE OF REPORTING PERIOD.—The requirement under section 304(b) of the National Security Act of 1947, as added by subsection (a) of this section, shall apply to a covered employee that has entered into an employment agreement on or before the date of the enactment of this Act.
“(d) FIRST REPORTING REQUIREMENT.—The first report required to be submitted by each former covered employee under section 304(c) of the National Security Act of 1947, as added by subsection (a) of this section, shall be submitted not later than one year after the date of the enactment of this Act.
“(e) INITIAL REPORT REQUIREMENT.—The Director of National Intelligence shall submit to the congressional intelligence committees the initial list of foreign governments under section 304(d) of the National Security Act of 1947, as added by subsection (a) of this section, not later than 30 days after the date of the enactment of this Act.
“(f) TABLE OF CONTENTS.—The table of contents in the first section of such Act is amended—
“(1) by striking the second item relating to section 302 (Under Secretaries and Assistant Secretaries) and the items relating to sections 304, 305, and 306; and
“(2) by inserting after the item relating to section 303 the following new item:
“Sec. 304. Restrictions on certain former intelligence officers and employees.

AMENDMENT NO. 5 OFFERED BY MR. KELLY OF ILLINOIS

At the end of subtitle A of title III, add the following new section:

SEC. 304. RESTRICTIONS ON CERTAIN FORMER INTELLIGENCE OFFICERS AND EMPLOYEES.

Section 1024 of the National Security Act of 1947 (50 U.S.C. 2324) is amended—

(1) in subsection (c)(1), by inserting ‘‘and Predominantly Black Institutions’’ after ‘‘universities’’; and

(2) in subsection (g)—

(A) by redesignating paragraph (4) as paragraph (5); and

(B) by inserting after paragraph (3) the following new paragraph:

“(4) PREDOMINANTLY BLACK INSTITUTION.—The term ‘Predominantly Black Institution’ has the meaning given the term in section 318 of the Higher education Act of 1965 (20 U.S.C. 1058).

AMENDMENT NO. 6 OFFERED BY MR. CARNEY OF DELAWARE

At the end of subtitle B of title III, add the following new section:

SEC. 304. REPORT ON DECLASSIFICATION PROGRESS.

Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to Congress a report describing—

(1) how to improve the declassification process across the intelligence community; and

(2) what steps the intelligence community can take, or what legislation may be necessary, to enable the Central Intelligence Agency to better accomplish the missions assigned to the Center by Executive Order 13526.

AMENDMENT NO. 10 OFFERED BY MS. JACKSON OF TEXAS

At the end of subtitle B of title III, add the following new section:

SEC. 304. DIRECTOR OF NATIONAL INTELLIGENCE STUDY ON THE USE OF CONTRACTORS IN THE CONDUCT OF INTELLIGENCE ACTIVITIES.

The Director of National Intelligence shall conduct an assessment of the reliance of intelligence activities on contractors to support Government activities, including an assessment—

(1) contractors performing intelligence activities (including intelligence analysis); and

(2) the skills performed by contractors and the availability of Federal employees to perform those skills.

AMENDMENT NO. 11 OFFERED BY MR. KEATING OF MASSACHUSETTS

At the end of subtitle B of title III, add the following new section:

SEC. 304. ASSESSMENT OF THE EFFICACY OF MEMORANDA OF UNDERSTANDING TO FACILITATE INTELLIGENCE-SHARING.

Not later than 90 days after the date of the enactment of this Act, the Under Secretary of Homeland Security for Intelligence and Analysis, in consultation with the Director of the Federal Bureau of Investigation and the Program Manager of the Information Sharing Environment, shall submit to the congressional intelligence committees, the Committee on Homeland Security of the House of Representatives, and the Committee on Homeland Security and Governmental Affairs of the Senate an assessment of the efficacy of the memoranda of understanding between Federal, State, local, tribal, and territorial agencies to facilitate intelligence-sharing within and separate from the Joint Terrorism Task Force. Such assessment shall include—

(1) any language within such memoranda of understanding that prohibited or may be construed to prohibit intelligence-sharing between Federal, State, local, tribal, and territorial agencies; and

(2) any recommendations for memoranda of understanding to better facilitate intelligence-sharing between Federal, State, local, tribal, and territorial agencies.

The CHAIRMAN. Pursuant to House Resolution 604, the gentleman from Michigan (Mr. ROGERS) and the gentleman from Maryland (Mr. RUPPERSBERGER) each will control 10 minutes.

The Chair recognizes the gentleman from Michigan.

Mr. ROGERS of Michigan. Mr. Chairman, I yield myself such time as I may consume.

Mr. Chairman, I urge the committee to adopt the amendments en bloc, all of which have been examined by both the managers and the minority. I believe these amendments to be noncontroversial, and intended to enhance the underlying bill.

The manager's amendment is intended to make minor technical modifications to clarify two provisions that were added in markup.

I have an amendment that would require employees at senior level in the intelligence community to endure a “cooling off” period before being employed by a company that is owned or controlled by a foreign government that poses a high counterintelligence threat. It would also make them subject to reporting procedures.

This amendment stems from my concern that some senior level employees in the intelligence community retire or otherwise separate from the U.S. Government and take employment with foreign companies or foreign-controlled companies after holding positions where they likely learned very sensitive information that would be of value to those particular companies or governments.

It is not intended to be punitive prohibition on post-intelligence community employment but rather to establish a procedure to establish that sufficient time has lapsed to avoid conflicts of interest or the appearance of impropriety.

Mr. CARNEY has an amendment that would provide the Congress with a useful report on ways to improve the declassification process across the intelligence community. The intelligence community has declassified a massive amount of documents. Increased transparency through an improved declassification process will help rebuild the confidence of the American people in their intelligence agencies.

Mr. CONNOLLY has an amendment that will add several best practices to the assessment our bill requires for intelligence community software licenses. This amendment is all the more important in light of current efforts to improve the intelligence community information technology systems. Wise management of software licenses can help save the taxpayers’ dollars while making sure our intelligence officers have the tools they need to do their job.

Ms. JACKSON LEW has an amendment that will help us identify ways to improve the support contractors offer to the intelligence community. It may help us find ways to make the most of scarce resources, all while ensuring that the contractors perform inherently governmental functions.

Mr. KEATING has an amendment concerning intelligence sharing between
Federal, State, and local entities, which has been a critical tool to prevent terrorist attacks on American soil. Joint terrorism task forces pool talent, skills, and knowledge from across the law enforcement and intelligence communities into a single entity that can respond with the flexibility and speed to stop impending threats.

Even so, we must always look for ways to improve intelligence-sharing relationships. This amendment requires a study of the efficiency of the memoranda of understanding signed between Federal, State, local, tribal, and territorial agencies. The study will help identify any obstacles to intelligence sharing between agencies and find improvements to existing intelligence-sharing relationships.

Ms. KELLY has an amendment to expand a grant program by the Director of National Intelligence to include predominantly black institutions. To succeed in this mission, the intelligence agencies need our Nation’s top talent, and that means they must make full use of our Nation’s diverse population. These grants will help provide study programs in foreign languages such as Farsi, Pashto, Middle Eastern, South Asian, and African dialects. Foreign language skills are critical for intelligence officers, as we all know.

Mr. RUPPERSBERGER has an amendment that will require the intelligence community Chief Information Officer to make recommendations to the Director of National Intelligence based on the software licensing assessment required by section 307 of the bill. It will also require the DNI to issue guidelines to implement those recommendations. These recommendations and guidelines will help the IC implement the results of the important assessment that this bill will require regarding software licensing.

I will, therefore, support the amendment.

With that, Mr. Chairman, I ask Members to support my bill this evening, and I reserve the balance of my time.

Mr. RUPPERSBERGER. Mr. Chair, I yield myself such time as I may consume.

I support all these amendments.

I agree with Chairman ROGERS that it is very troubling when senior U.S. officials who know our most sensitive secrets leave the Federal Government and immediately go to work for a company that is owned by a foreign country to do the type of work that should be done by U.S. Government employees.

I agree with Ms. ROBIN KELLY that we need to increase the diversity of our intelligence workforce by adding predominantly black institutions to ongoing intelligence community programs currently designed for Historically Black Colleges and Universities. It is a good thing in its own right, and it will create even greater opportunities for intelligence collection.

I agree with Mr. CARNEY that we must reduce our declassification backlog. As The New York Times reported just this week, even material that should be automatically declassified isn’t. So we need the Director of National Intelligence to look across the intelligence community and figure out how to improve the declassification process so that more national security information can be made available to the American people now.

I also agree with Ms. SHEILA JACKSON LEE that we need to get a handle on how we are employing our contractors. We need to know whether they are doing the type of work that should be done by U.S. Government employees.

Let me be clear, however, that contractors perform a very valuable service, and our companies are among the very best in the world. But there needs to be a clear line between what we expect from our employees, who owe 100 percent of their loyalty to the government, and what we expect from our contractors, whose patriotism is without question, but whose loyalty is also to the company that employs them.

Finally, I agree with Mr. KEATING, Mr. ROONEY, and Mr. HANNA that we need to take a close look at the memos that agree between the Federal Government and the State, local, tribal, and territorial governments to make sure they are written clearly enough and well enough to ensure the free flow of intelligence, while still making sure to protect sources and methods.

Intelligence is critical, particularly in the midst of a domestic crisis. And for it to be useful, it must get to those who need it.

In addition to the manager’s amendment, which makes technical and clarifying changes to the bill, I support all these amendments.

I reserve the balance of my time.

Mr. ROGERS of Michigan. Mr. Chairman, I reserve the balance of my time.

Mr. RUPPERSBERGER. Mr. Chair, I yield 2 minutes to the gentlewoman from Texas (Ms. JACKSON LEE).

Ms. JACKSON LEE of Texas. Mr. Chair, let me again thank the ranking member and the chairman. Let me also acknowledge the work of our men and women who work in our intelligence community in the United States and around the world.

I would like to thank the House Permanent Select Committee on Intelligence for their efforts to include the Jackson Lee amendment in the en bloc amendments and thank them for working with my staff in a very cooperative manner.

The Jackson Lee amendment seeks greater transparency to Congress on the people the Nation relies upon to perform certain types of work for the intelligence community.

This Jackson Lee amendment requires the Director of the Office of National Intelligence to conduct an assessment of the reliance of intelligence activities on contractors to support government objectives, including an assessment of contractors performing intelligence activities, which would include intelligence analysis.

This complements the underlying bill, because the underlying bill has determined to assess the utilization and reduce the number of private contractors.

In a Time article dated Monday, July 19, 2010, a comment says:

Explosion of contractors in the intelligence community.

And that has been the case.

It is important that we recognize that contractors can be useful. But like the President stated publicly on August 26, 2013:

It is important that we have so many extraordinarily capable folks in our military and our government who can do this—and probably do it cheaper.

Well, I agree with the President and this committee.

I also take note of an article that cites NSA contractors using LinkedIn profiles to cash in on national security.

I believe that with the work that we are doing here in this legislation, along with my amendment, we will get our hands around the idea of outsourcing our intelligence work and develop a pathway of excellence, as we have in the past.

We will utilize our veterans, we will utilize military personnel, we will utilize young persons who are interested in this as a career, and we will have the finest intelligence staffing that we have ever had, as we have had in the past.

I ask my colleagues to support this amendment. I again thank the chairman and ranking member for including this in the en bloc amendments. I think we are on a pathway of greater success in securing this Nation.

Mr. Chair, I support H.R. 4681, the “Intelligence Authorization Act for Fiscal Years 2014,” a bill Authorizing appropriations for our Nation’s intelligence agencies for Fiscal Year 2014 through Fiscal Year 2015. The bill provides funds for the conduct of intelligence and intelligence-related activities.

My thanks to the House Rules Committee for making my amendment in order under the rule for H.R. 4681. I appreciate the work of the House Permanent Select Committee on Intelligence efforts to include the Jackson Lee Amendment in the En Bloc.
My amendment is simple and makes an important contribution to the bill.

The Jackson Lee Amendment seeks greater transparency to Congress on the people the nation relies upon to perform certain types of work for the Intelligence Community.

The Jackson Lee Amendment requires the Director of the Office of National Intelligence to conduct an assessment of the reliance of intelligence activities on contractors to support Government objectives, including an assessment of contractors performing intelligence activities, which would include intelligence analysts.

The Office of the Director of National Intelligence (ODNI) 2013 Report on Security Clearance Determinations said that on October 1, 2013, the total number of persons with a Confidential, Secret or Top Secret security clearance totaled 5,150,379 individual.

According to the ODNI, 3,738,026 were government agency personnel, 1,056,309 were contractors and 356,044 were categorized as other.

Between January and October 1, 2013 there were 777,168 security clearances approved—152,490 were government agency employees and 131,209 were contractors with an additional 12,785 designated as other.

The cost of government security classification in 2005 was $7.66 billion and in 2011 the total was $22.6 billion.

The amount expended included: 5.65 billion for protection maintenance; 1.53 billion for security management oversight and planning; 502.51 million for professional education, training and awareness; 352.4 million for classification management; 52.76 million for declassification.

The assessment provided for through the Jackson Lee amendment would shed light on the work that our federal agency Intelligence professionals and the role contractors play in protecting our nation.

President Obama stated publicly on August 6, 2013 that it is important that we have so many ‘extraordinarily capable folks in our military and our government who can do this, and probably do it cheaper.’

I agree.

That is why I introduced H.R. 4110, the HERO Transition from Battlespace to Workplace Act of 2014.

This legislation addresses the problem of underemployed veterans in obtaining positions that take maximum advantage of their skills and experience.

For some time I have worked to make sure that transparency, accountability and oversight were firmly established to guide the work of intelligence agencies, including introducing legislation such as H.R. 2404.

I thank my colleagues on the Intelligence Committee for their hard work in bringing this bill before the full House for consideration. I ask my colleagues in the House to vote for this en bloc.

[From Time, Jul. 19, 2010]

TIME To TAME WASHINGTON’s INTELLIGENCE BEAST

(By Robert Baer)

I asked a former colleague who retired from the CIA not long ago what he thought about the Washington Post article Monday, July 19, on the explosion of contractors in the intelligence community. “It’s a horror,” he said, “my tax money blowing around Washington like confetti.” But he reserved his angrier comments for the contractor-driven bureaucracy that allowed a Nigerian would-be suicide bomber—as alleged by a resulting federal indictment—to board a Northwest flight from Lagos to Detroit in December. In spite of the billions and billions of dollars we’ve showered on contractors, consultants and corporate contracts since 9/11, no one managed to disseminate a warning from the Nigerian’s father that his son had reportedly become a terrorist.

The raw numbers tell the story. Since 9/11, America’s intelligence budget has more than doubled, to $76 billion. The number of people working at the Defense Intelligence Agency (DIA) has increased from 7,700 troops to 16,500. The FBI’s Joint Terrorism Task Forces have trebled in number, rising from 35 to 106. Personnel at the National Security Agency has doubled. There are 85,000 people with top-secret security clearances, including contractors—almost 1/3 times the population of Washington. It shouldn’t come as a surprise, then, that the Nigerian slipped through the cracks: there are so many more cracks now. But we shouldn’t reduce the problem to our having become a country saddled with a bureaucratic quagmire of timeservers and people cashing in on 9/11. Recently I’ve been giving talks at government agencies working on counterterrorism. With almost no exceptions, I’ve found my audiences, including contractors, better informed, more dedicated and better educated than the generation I served with in the CIA. (As I’ve said to the CIA today, I wonder whether I’d make it in.) The problem is that I came away from these talks with the impression that the post-9/11 workforce is bored and even adrift—at least in the sense that there are too many people chasing too little hard intelligence.

It’s a tooth-to-tail problem. CIA Director Leon Panetta has gone on the record as saying there are only a couple hundred al-Qaeda dead-enders in the mountains between Pakistan and Afghanistan, most of whom are dormant, hiding in caves. With a prey so small and elusive and a bureaucracy so dormant, hiding in caves. With a prey so small and elusive and a bureaucracy so small and dormant, and even adrift—at least in the sense that there are so many more cracks now...
Mr. Chairman, it is important to note that my amendment does not task another Federal agency with the responsibility of determining our vulnerabilities to EMP and GMD and the potential dangers these threats represent to our nation.

These studies have already been finalized, and their conclusions provide our Nation’s leaders and industry officials with the clarity they need to move forward toward protecting our grid.

In fact, Mr. Chairman, there have now been nearly a dozen Federal Government reports and studies on the dangers, threats, and vulnerabilities the U.S. electric grid faces from EMP and GMD, including reports from the EMP Commission, Department of Homeland Security, Department of Defense, Department of Energy, the Federal Energy Regulatory Commission, the National Academy of Sciences, and the U.S. national laboratories. All of them come to similar conclusions: The U.S. electric grid is dangerously vulnerable to EMP and GMD.

Further, many warn that, given the Nation’s current lack of preparedness, a nuclear or natural EMP event is potentially the most catastrophic threat that would be a top national priority for our national security and homeland security.

In 2008, the congressionally authorized EMP Commission stated that Russian scientists had proliferated knowledge of a specifically designed EMP weapon to North Korea. There may also exist a form of mobile EMP devices that can take out our electric substations.

As The Wall Street Journal reported recently, taking out just a few of these substations simultaneously could potentially cause a nationwide blackout.

Our military understands this threat very well, Mr. Chairman, and has protected many of our critical defense assets. We, as a Nation, have spent billions of dollars, in fact, over the years, hardening our nuclear triad, our missiles, defense capabilities and numerous other critical elements of our national security apparatus against the effects of electromagnetic pulse, particularly the type of electromagnetic pulse that might be generated against us by an enemy.

However, our civilian grid, which the Department of Homeland Security estimates relies on for nearly 99 percent of its electricity needs, is completely vulnerable to the same kind of danger.

This constitutes, in my opinion, Mr. Chairman, an invitation on the part of certain of our enemies to use the asymmetric capabilities of an EMP weapon against us, and there is now evidence that such strategy is being considered by certain of those enemies.

Mr. Chairman, the time is right for this action, and our efforts today may gain us no note in the annals of history, but my hope is that they will ultimately lead to a time when this country mitigates this threat and disinvites our enemies to try to exploit it against us. I pray it happens just that way.

Mr. Chairman, I yield back the balance of my time.

Mr. RUPPERSBERGER. Mr. Chairman, I yield myself such time as I may consume.

Mr. FRANKS, a leader in the bipartisan House Electromagnetic Pulse Caucus, has brought attention to the serious threats posed by electromagnetic pulses, whether from a solar storm or a nuclear-armed enemy that could harm our critical infrastructure.

Given what we know about our Nation’s critical infrastructure vulnerabilities, I support this amendment’s purpose, to gain even more information that can better protect our utilities, financial systems, medical facilities, networks, and other infrastructure.

Therefore, I support this amendment, and I urge my colleagues to do the same.

Mr. Chairman, I yield 2 minutes to the gentleman from Rhode Island (Mr. Langevin), one of the key members of our committee and one of the experts in the area of cybersecurity.

(Mr. Langevin asked and was given permission to revise and extend his remarks.)

Mr. Langevin. Mr. Chairman, I rise in support of H.R. 4681, the Intelligence Authorization Act for Fiscal Years 2014 and 2015.

I am going to keep my remarks brief, but I first wanted to thank Chairman Rogers and Ranking Member Ruppersberger for bringing this bill to the floor in a bipartisan way. The bill before us really is indicative of how the committee is run in a bipartisan way under Chairman Rogers’ leadership.

In particular, I do want to commend Chairman Rogers for his years of service on the Intelligence Committee and wish him the best in his retirement at the end of this year. He clearly made a difference.

Mr. Chairman, this is a balanced measure and really critical to protecting our Nation’s security. I have been pleased to work with the chairman and ranking member on several provisions included in the bill.

This bill makes critical investments in technical and tactical intelligence, as well as in our human capabilities.

In particular, in order to support and develop the long-term health of our most important intelligence resource—human talent—this bill requires the Director of National Intelligence to create a plan to promote cybersecurity and computer literacy among high school and college students.

As cyber threats grow in quantity and sophistication, we must do more to train and recruit into the noble calling of government service young people with the interest and aptitude for cybersecurity.

The bill authorizes provisions to reduce the risk of information leaks, as well, and unauthorized disclosures of classified information by insiders, while maintaining appropriate levels of trust in our personnel. We cannot afford a repeat of last year’s breach of classified information.

Mr. Chairman, continued focus is needed to ensure that we, of course, are supporting the efforts of the patriotic Americans who proudly serve our Nation in the intelligence community, while properly safeguarding the privacy and civil liberties that our citizens hold dear.

To that end, we must fully absorb the lessons learned over the past decade after passage of the landmark Intelligence Reform and Terrorism Prevention Act and the changes it brought to the IC.

The Acting Chair. The time of the gentleman has expired.

Mr. Ruppersberger. I yield the gentleman an additional 1 minute.

Mr. Langevin. I certainly look forward to working with my committee colleagues to continue this tradition of rigorous, responsible, and bipartisan oversight. The work that we do is critical to our national security.

Again, I thank Chairman Rogers and Ranking Member Ruppersberger, as well as my colleagues on the committee, and in particular, I want to thank the staff for the hard work that they have done in bringing this bill to the floor on both sides of the aisle. Their work is critical as well.

I thank my colleagues.

Mr. Ruppersberger. Mr. Chairman, I yield back the balance of my time.

The Acting Chair. The question is on the amendment offered by the gentleman from Arizona (Mr. Frank).

The amendment was agreed to.

Amendment No. 7 Offered by Mr. Poe of Texas

The Acting Chair. It is now in order to consider amendment No. 7 printed in House Report 113–465.

Mr. Poe of Texas. Mr. Chairman, I have an amendment at the desk.

The Acting Chair. The Clerk will designate the amendment.

The text of the amendment is as follows:

At the end of subtitle B of title III, add the following:

SEC. ___ REPORT ON UNITED STATES COUNTER-TERRORISM STRATEGY TO DISRUPT, DISMANTLE, AND DEFEAT AL-QAEDA, ITS AFFILIATED GROUPS, ASSOCIATED GROUPS, AND ADHERENTS.

(a) Report.—

(1) In general.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the appropriate committees of Congress a comprehensive report on the United States counterterrorism strategy to disrupt, dismantle, and defeat al-Qaeda, its affiliated groups, associated groups, and adherents.
The Acting CHAIR. Pursuant to House Resolution 604, the gentleman from Texas (Mr. POE) and a Member objected each will control 5 minutes.

Mr. POE of Texas. Mr. Chairman, I would like to thank Chairman ROGERS for supporting this amendment but, more importantly, for his work on the Intelligence Committee for so many years and, prior to that, your work with the FBI.

As a former judge, I got to see a lot of FBI agents come and testify in Texas, and they had a wonderful reputation. You also have that reputation, and thank you for your service in law enforcement and in the House. I also want to thank the ranking member for his support, generally, for this amendment.

This amendment requires the Director of National Intelligence, in coordination with relevant agencies, to produce a strategy to defeat al Qaeda and its affiliates.

The amendment requires that the President clearly define groups like core al Qaeda and al Qaeda affiliates and other terms the administration uses to define this enemy of America.

Al Qaeda continues to threaten the security of the United States and our allies, both here at home and abroad. Our intelligence services and our military have scored some real gains against al Qaeda, but al Qaeda in Afghanistan and Pakistan is still able to provide technical, tactical, and strategic direction to its affiliates throughout the world.

Al Qaeda has gone from on the verge of strategic defeat to a serious and growing threat, depending on who you ask in our intelligence services or even the administration. Today, al Qaeda controls more territory than it ever has. The fight against al Qaeda is far from over, and it will continue to grow.

As chairman of the House Foreign Affairs Subcommittee on Terrorism, Nonproliferation, and Trade, I have held over a dozen bipartisan hearings focusing on this very topic. Once again, I want to thank the chairman and ranking member for including this TNI Subcommittee in some of the work we have done together on the very issue of intelligence.

During these 12 hearings in our subcommittee, we have yet to find a witness who can articulate or even agree with the administration’s counterterrorism strategy or what it is or describe how the administration really views al Qaeda and its threat. This seems to be a problem. This needs to be clarified, so that all of us know exactly what our strategy is nationwide and worldwide.

So this amendment is necessary, so we can all get on the same page in the hymnal with a clear strategy to defeat al Qaeda, so we understand what al Qaeda is really doing today in 2014. This is a constantly changing movement, and al Qaeda today isn’t the same as the al Qaeda in 2001.

We need to have a clear understanding of who we are fighting and how we are going to defeat the al Qaeda terrorists. Drone strikes and targeted killings are not a strategy; they are tactics. Therefore, I support this amendment, and I urge support by the committee and the whole House.

And that’s just the way it is.

Mr. Chairman, I yield back the balance of my time.

Mr. RUPTERSBERGER. Mr. Chairman, I claim the time in opposition, although I am not opposed to the amendment.

The Acting CHAIR. Without objection, the gentleman from Maryland is recognized for 5 minutes.

There was no objection. Mr. RUPTERSBERGER. I yield myself as much time as I may consume.

I support this amendment because the time is right to step back and take stock of where we are and how we are doing in our fight against terrorism. The threat is not going away, but it is rapidly changing.

The Director of the FBI, Jim Comey, recently said that the terrorism threat is very much alive and growing in new and more dangerous places around the world. It even surprised him when he started, just how virulent and dispersed the terrorist threat had become.

From Pakistan to Yemen, Afghanistan, to Syria, north Africa to Iraq, the threat from al Qaeda is waxing in some areas, but growing in others. Unless we approach this dangerous problem holistically and precisely, we risk just squeezing the balloon, suppressing terrorism in one area, only to see it grow elsewhere.

So I think it is a good idea to sit down and take a comprehensive look at the problem today, to make sure that we are confronting it in the precisely right way, to make sure that we are designing our effectiveness correctly, and to make sure that we have the right and most current legal authorities.

Mr. Chairman, I yield back the balance of my time.

The Acting CHAIR. The question is on the amendment offered by the gentleman from Texas (Mr. Poe).

The amendment was agreed to.

AMENDMENT NO. 9 OFFERED BY MR. GALLEGO

The Acting CHAIR. It is now in order to consider amendment No. 9 printed in House Report 113–465.

Mr. GALLEGOS. Mr. Chairman, I have an amendment at the desk.

The Acting CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

At the end of subtitle B of title III, add the following section:

SEC. 2. REPORT ON RETRAINING VETERANS IN CYBERSECURITY.

Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence, in consultation with the Secretary of Defense, the Secretary of Veterans Affairs, and the Secretary of Homeland Security, shall submit to Congress recommendations for retraining veterans and retired members of elements of the intelligence community in cybersecurity.

The Acting CHAIR. Pursuant to House Resolution 604, the gentleman from Texas (Mr. GALLEGOS) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentleman from Texas.

Mr. POE of Texas. Mr. Chairman, I would like to thank Chairman ROGERS for supporting this amendment but,
Mr. GALLEG0. Mr. Chairman, I would like to begin by thanking Chairman ROGERS and the ranking member for an opportunity to work on this issue with them, and I certainly wish Chairman ROGERS well in his future endeavors.

Mr. Chairman, this amendment helps us find ways to ensure that our veterans and other former public servants can continue their service to our country on cybersecurity, a critical national security need that will only grow in importance over the next several years.

While Congress is well aware of the challenges that we face in cybersecurity, it is important to understand that cyber attacks are not only aimed at the government, where they challenge our national security and endanger our troops, but these attacks also target our Nation’s economic advantages, our core advantages, when they steal proprietary information and intellectual property from American firms that lead the Nation and lead the world in innovation.

In fact, for the private sector, it is important to know that an IP theft in the U.S. costs companies upwards of $250 billion a year, and global cyber crime costs $338 billion. And when you factor in downtime, either way, that is a lot of money. And we spent up to—no kidding—$1 trillion fixing these problems.

These highlight an important point, that if these attacks on American companies are so bad, just use your imagination to figure the threat of foreign based cyber attacks on the Department of Defense or other critical intelligence agencies. And there is no better group of people than our veterans and our retired members of the intelligence community who could be ready to assist in cybersecurity efforts.

This amendment allows us to do everything we can to support our veterans who are looking for jobs along with those retired members of the intelligence community who have already demonstrated their commitment to public service.

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

Mr. ROGERS of Michigan. Mr. Chairman, while I do not oppose the amendment, I ask unanimous consent to control the time in opposition.

The Acting CHAIR. Is there objection to the request of the gentleman from Michigan?

There was no objection.

The Acting CHAIR. The gentleman from Michigan is recognized for 5 minutes.

Mr. ROGERS of Michigan. Mr. Chairman, I yield myself such time as I may consume.

Our Nation owes a debt of gratitude to its veterans and to the retired members of the intelligence community. We should look for as many ways as possible to help them succeed in the job market. And I want to thank the gentleman for offering the amendment for promoting this. The amendment does, again, highlight the sheer level of threat we face from cyber crime, cyber terrorists, cyber espionage. We are being overwhelmed.

When you look at China, Russia, Iran, and now organized crime groups who are approaching nation-state capability, it is as bad as I have ever seen it. And, again, 85 percent of the networks across America are not protected at all because they are private sector networks. The government, itself, is about 15 percent of those networks.

We need to find a pathway, A, to attract the talent that the gentleman from Texas (Mr. GALLEG0) is talking about; and, B, we need to allow these private sector folks to protect themselves by gaining information, sharing information the government has that could protect those networks from cyber threats.

It is happening each and every day. The next generation of cyber warriors are there. And I think this amendment will go a long way to recruit the right talent in the right place to help us meet this growing threat of the future, one of prosperity, safety, and the security of the United States.

With that, I yield back the balance of my time.

Mr. GALLEG0. Mr. Chairman, I yield 1 1/2 minutes to the gentleman from Maryland (Mr. RUPPERSBERGER).

Mr. RUPPERSBERGER. Mr. Chairman, I support this amendment, and I urge my colleagues to do the same.

As I said in the opening hearing on worldwide threats, ‘education is the keystone of security and prosperity in the 21st century.’

The cyber threats we face are grave, and we need to train the best, the brightest, and the most dedicated—like our military veterans and our retired intelligence professionals—to be our next generation of cyber defenders. We call them cyber warriors.

Everyday, we hear about cyber attacks in the news. Early last year, for example, our financial sector suffered a wide-scale network denial of service attack that proved difficult and very costly to mitigate. The retail giant, Target, is another recent example of our vulnerability to cyber attacks. And today, the Washington Post stated that Iranian hackers are targeting U.S. officials through social networks.

We need to pass cybersecurity legislation like CISPA, and we need to do much, much more to expand our bench of cyber professionals and innovators. We need to invest in early education in science, technology, engineering, and math. And we equally need to leverage the experience and wisdom of our veterans and former intelligence professionals. Our amendment does not ask Washington to fund heavy investments in cyber education. We must do the same. For this reason, I support this amendment.

I thank my colleague from Texas (Mr. GALLEG0) for his amendment. He represents the area of Texas that is close to the border. He understands the threat and why we need intelligence to deal with national security.

Mr. GALLEG0. Mr. Chairman, many of our servicemembers have made the ultimate sacrifice. There are 4,223 that have died in Operation Iraqi Freedom; 66 in Operation New Dawn; and, as of yesterday, 2,330 have died in Operation Enduring Freedom in Afghanistan, where I just returned from this week.

But many of the thousands upon thousands of our troops who did make it home to see their mothers, fathers, spouses, and kids are alive today because actionable intelligence helped them achieve their missions more safely.

While there has been a lot of criticism about intelligence collection—and we have had a very robust debate on these issues—I think it is important that we concentrate on the fact that intelligence is so critical to the lives of our men and women in uniform. And it really helps help our all-volunteer force come back home today safe with their families because of the work of our numerous intelligence agencies who have provided the information they need to stay alive.

Mr. Chairman, I also want to do a shout-out to the Air Force ISR Agency in San Antonio, in Bexar County. I know that they do critical work to protect and defend our liberty each and every day.

Mr. Chairman, I yield back the balance of my time.

The Acting CHAIR. The question is on the amendment offered by the gentleman from Texas (Mr. GALLEG0).

The amendment was agreed to.

The Acting CHAIR. The question is on the amendment in the nature of a substitute, as amended.

The amendment was agreed to.

The Acting CHAIR. Under the rule, the Committee rises.

Accordingly, the Committee rose; and the Speaker pro tempore (Mr. POE of Texas) having assumed the chair, Mr. WOMACK, Acting Chair of the Committee of the Whole House on the state of the Union, reported that that Committee, having had under consideration the bill (H.R. 4681) to authorize appropriations for fiscal years 2014 and 2015 for intelligence and intelligence-related activities of the United States Government, the Community Management Account, and the Central Intelligence Agency Retirement and Disability System, and for other purposes, and, pursuant to House Resolution 604, he reported the bill back to the House with an amendment adopted in the Committee of the Whole.

The SPEAKER pro tempore. Under the rule, the previous question is ordered.

Is a separate vote demanded on any amendment to the amendment reported from the Committee of the Whole?

If not, the question is on the amendment in the nature of a substitute, as amended.
The amendment was agreed to. The SPEAKER pro tempore. 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.

MOTION TO RECOMMIT
Mr. BISHOP of New York. Mr. Speaker, I have a motion to recommit the bill.

The SPEAKER pro tempore. Is the gentleman opposed to the bill?

Mr. BISHOP of New York. In its current form, I am.

The SPEAKER pro tempore. The Clerk will report the motion to recomit.

The Clerk read as follows:

Mr. Bishop of New York moves to recommit the bill, H.R. 4681, to the Permanent Select Committee on Intelligence with instructions to report the same back to the House forthwith with the following amendment:

At the end of subtitle A of title III, add the following new section:

SEC. PROTECTING UNITED STATES MILITARY TECHNOLOGY AND INDUSTRIAL COMPETITIVENESS FROM CHINESE AND OTHER STATE-SPONSORED COMPUTER THEFT.

The head of each element of the intelligence community shall—

(1) prioritize efforts to uncover and foil attempts to steal United States military technology, and the intellectual property of United States corporations, by State-sponsored computer hackers from China and other foreign countries;

(2) consistent with existing law, immediately inform corporations and Internet providers when network breaches occur, collaborate with Federal agencies to protect critical infrastructure, and assist law enforcement, as well as our international partners in apprehending, halting, and punishing those who infiltrate our systems.

The intelligence agencies are also required to notify businesses and Internet providers when network breaches occur, collaborate with Federal agencies to protect critical infrastructure, and assist law enforcement, as well as our international partners in apprehending, halting, and punishing those who infiltrate our systems.

The need for this amendment is clear: Growing evidence reveals extensive activity on the part of the People’s Liberation Army to conduct cyber, economic, and industrial espionage. Their hacking knows no bounds in the pursuit of state and trade secrets alike. We have seen the traces and telltale signs of hacking into Federal systems and U.S. corporations, like Alcoa, U.S. Steel, energy companies like SolarPowerAG, and even nuclear power providers like Westinghouse Electric Company.

This month, the Justice Department indicted five members of the Chinese military for stealing trade secrets in order to prosper from American ingenuity and innovation to undercut our global competitiveness.

These are not isolated incidents. The frequency of these attacks has increased over time, costing our economy thousands of jobs and up to $100 billion annually. Not only are the Chinese and their partners indiscriminate—refusing to acknowledge evidence we have uncovered, but they refuse to negotiate steps both of our nations could pursue to end this threat.

No one single action will stop the Chinese from attempting to infiltrate American computer networks, but collaboration between our intelligence agencies, law enforcement, and the private sector can strengthen our defenses, deter cyber espionage from being launched on foreign soil, and protect our jobs.

My amendment is not the only step we can take, but it is an important addition to this bill. The United States deserves better for supporting the rights of nations like China to trade in the global marketplace, to be treated with respect, and to participate in the community of nations. We must send the message to China and our rivals that this Congress stands ready to defend our national security and our economy, and we must send a message to foreign states that Americans that protecting jobs here at home will always be our priority and that our economic might is more important than our military might. Our national security and position as a global leader in innovation and competitiveness depends on it.

Mr. Speaker, I urge my colleagues to support this amendment.

I yield back the balance of my time.

Mr. ROGERS of Michigan. Mr. Speaker, I rise in opposition to the motion to recommit.

The SPEAKER pro tempore. The gentleman is recognized for 5 minutes.

Mr. ROGERS of Michigan. Mr. Speaker, I thank the gentleman for his interest. This is exciting news.

The bill is not drafted correctly, and it opens us up to exposing classified information to corporations that may be foreign-owned and operated by the very counterintelligence threat we seek to push back on. But thank you for your effort.

We should reject this. We should include resounding support for the CISPA bill that carefully drafted language to make sure that there is a cyber-sharing relationship, both between the government when it comes to malicious code and the private sector who, remember, is all by itself out there getting attacked by nation-states and large organized criminal groups trying to steal their information.

If you think about even the last month or so that General Alexander was the Director of the National Security Agency, just in that last bit of time he was there, the military sites, the government sites were hit 41 million times by people trying to cause destruction or break in and steal something. Again, this is as serious a problem as you can imagine, Mr. Speaker, that we are not prepared to handle.

So that CISPA bill that I think you tried to get here—I mean, part of this bill is the redundancy department of redundancy. The second part is just not drafted correctly, and we would love to help you get to the right place.

I think, this bill, I think it would all be more harm than I think you realized without carefully considering how you construct a cyber-sharing malicious code relationship between the government and the private sector. It needs to happen this way, it just exposes, again, the information to counterintelligence groups that we don’t want to have it.

So I would strongly urge the rejection of the motion to recommit. But I want to thank the gentleman, I look forward to working in the next few months with the gentleman to make sure that we put in place a fighting chance, a fighting chance for the 85 percent of those private sector networks that are getting absolutely ravaged every single day by cyber attackers, by people who are trying to disrupt activities.

1115

There are public reports that Iran is probing our financial institutions. Think about the idea if they were able or successful to go in and take down a financial institution that has trillions
May 30, 2014

CONGRESSIONAL RECORD — HOUSE

of dollars every single day in global transactions, destroy data, manipulate data, and you don’t know who owes whom what. Imagine the economic catastrophe that happens.

Well, guess what? This is not Orwellian. It is not next year. It is not 6 months from now, and it is not 10 years from now. It is happening today, and every nation on the face of the Earth is trying to get this capability—including al Qaeda. They are advertising to try to find the right people to develop a capability for a cyberattack to disrupt, to destroy, and to cause chaos.

This is as important an issue as I can think of. Mr. Speaker, that I hope we find some resolution on. Again, I have forward to working with the gentleman on the CISPST bill that is in the Senate and passed by this House in a huge bipartisan way so that we can bring relief and security to the future prosperity of the United States of America.

With that, I yield back the balance of my time.

The SPEAKER pro tempore. Without objection, the previous question is ordered on the motion to recommit.

There was no objection.

The SPEAKER pro tempore. The question was taken; and the Speaker pro tempore announced that the ayes had it.

Mr. BISHOP of New York. Mr. Speaker, on that I demand the yeas and nays.

The vote was taken by electronic device, and there were—yeas 345, nays 59, not voting 27, as follows: [Roll No. 271]

AYES—345

[Names of Members]

NAYS—220

[Names of Members]
Mrs. CAROLYN B. MALONEY of New York changed her vote from “aye” to “no.”

So the bill was passed.

The result of the vote was announced as above recorded.

A motion to reconsider was laid on the table.

REPORT TO CONGRESS TO LEARN MORE ABOUT THIS MOVEMENT AND ITS PROGRESS.

HONORING REBECCA MARTIN

Mr. BARROW of Georgia asked and was given permission to address the House for 1 minute and to revise and extend his remarks.

Mr. BARROW of Georgia. Mr. Speaker, I rise today to honor Rebecca Martin, the principal of Screven County Elementary School, who is retiring after more than 30 years as an educator.

Educators are the unsung heroes in the fight for a better life for all of us. Ms. Martin started her teaching career in 1981 and then went on to teach 18 years in the Screven County School System. Since becoming a principal in 1999, she has overseen a school system that has taught thousands of students who have received too many awards to be mentioned here, all as a direct result of her leadership and dedication to our children.

While I know the students and teachers of Screven County Elementary School will miss Ms. Martin’s spirit and dedication and she will miss seeing them as much as she is used to, she can be sure that her teaching and leadership have had a profound impact upon her students and her fellow teachers wherever they go.

I congratulate Ms. Martin on her retirement. I wish her; her husband, Dr. Charles Martin; their two children; and their six grandchildren all the good things to come in the next step of their journey together.

ACTION FOR DENTAL HEALTH

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

Mr. SIMPSON. Mr. Speaker, we are in the midst of a dental health crisis in this country. In 2010, 181 million Americans didn’t see a dentist. More than 50 percent of Americans over the age of 30 suffer from some form of periodontal disease, and estimates suggest that 25 percent of children under the age of 5 already have cavities.

It is time to take action. This is why the American Dental Association last year launched Action for Dental Health: Dentists Making a Difference, a nationwide, community-based movement focused on delivering care now to people already suffering from dental disease, strengthening and growing the public-private safety net to provide more care for more Americans, and bringing dental health education and disease prevention into underserved communities.

I urge all of my colleagues to read the Action for Dental Health One Year Report to Congress to learn more about this movement and its progress.

HONORING REBECCA MARTIN

Mr. BARROW of Georgia asked and was given permission to address the House for 1 minute and to revise and extend his remarks.

Mr. BARROW of Georgia. Mr. Speaker, I rise today to honor Rebecca Martin, the principal of Screven County Elementary School, who is retiring after more than 30 years as an educator.

Educators are the unsung heroes in the fight for a better life for all of us. Ms. Martin started her teaching career in 1981 and then went on to teach 18 years in the Screven County School System. Since becoming a principal in 1999, she has overseen a school system that has taught thousands of students who have received too many awards to be mentioned here, all as a direct result of her leadership and dedication to our children.

While I know the students and teachers of Screven County Elementary School will miss Ms. Martin’s spirit and dedication and she will miss seeing them as much as she is used to, she can be sure that her teaching and leadership have had a profound impact upon her students and her fellow teachers wherever they go.

I congratulate Ms. Martin on her retirement. I wish her; her husband, Dr. Charles Martin; their two children; and their six grandchildren all the good things to come in the next step of their journey together.

THE SPEAKER pro tempore (Mr. SIMPSON) said, pursuant to clause 1, rule I, the Journal stands approved.

AUTHORIZING THE CLERK TO MAKE CORRECTIONS IN EN-GROSSMENT OF H.R. 4681, INTEL-LIGENCE AUTHORIZATION ACT FOR FISCAL YEARS 2014 AND 2015

Mr. ROGERS of Michigan. Mr. Speaker, I ask unanimous consent that the Clerk be authorized to make such technical and conforming changes as necessary to reflect the actions of the House.

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

There was no objection.

ADJOURNMENT TO MONDAY, JUNE 2, 2014

Mr. ROGERS of Michigan. Mr. Speaker, I ask unanimous consent that the House adjourn today, adjournment to meet at noon on Monday, June 2, 2014.

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

There was no objection.

ACTION FOR DENTAL HEALTH

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

Mr. SIMPSON. Mr. Speaker, we are in the midst of a dental health crisis in this country. In 2010, 181 million Americans didn’t see a dentist. More than 50 percent of Americans over the age of 30 suffer from some form of periodontal disease, and estimates suggest that 25 percent of children under the age of 5 already have cavities.

It is time to take action. This is why the American Dental Association last year launched Action for Dental Health: Dentists Making a Difference, a nationwide, community-based movement focused on delivering care now to people already suffering from dental disease, strengthening and growing the public-private safety net to provide more care for more Americans, and bringing dental health education and disease prevention into underserved communities.

I urge all of my colleagues to read the Action for Dental Health One Year Report to Congress to learn more about this movement and its progress.

HONORING REBECCA MARTIN

Mr. BARROW of Georgia asked and was given permission to address the House for 1 minute and to revise and extend his remarks.

Mr. BARROW of Georgia. Mr. Speaker, I rise today to honor Rebecca Martin, the principal of Screven County Elementary School, who is retiring after more than 30 years as an educator.

Educators are the unsung heroes in the fight for a better life for all of us. Ms. Martin started her teaching career in 1981 and then went on to teach 18 years in the Screven County School System. Since becoming a principal in 1999, she has overseen a school system that has taught thousands of students who have received too many awards to be mentioned here, all as a direct result of her leadership and dedication to our children.

While I know the students and teachers of Screven County Elementary School will miss Ms. Martin’s spirit and dedication and she will miss seeing them as much as she is used to, she can be sure that her teaching and leadership have had a profound impact upon her students and her fellow teachers wherever they go.

I congratulate Ms. Martin on her retirement. I wish her; her husband, Dr. Charles Martin; their two children; and their six grandchildren all the good things to come in the next step of their journey together.