A motion to reconsider was laid on the table.

GENERAL LEAVE

Mr. GORDON of Tennessee. I ask unanimous consent that all Members may have 5 legislative days within which to revise and extend their remarks and include extraneous material on the bill, H.R. 4061.

The SPEAKER pro tempore (Ms. RICHARDSON). Is there objection to the request of the gentleman from Tennessee?

There was no objection.

CYBERSECURITY ENHANCEMENT ACT OF 2009

The SPEAKER pro tempore. Pursuant to House Resolution 1051 and rule XVIII, the Chair declares the House in the Committee of the Whole House on the State of the Union for the consideration of the bill, H.R. 4061.

□ 1254

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. 4061) to advance cybersecurity research, development, and technical standards, and for other purposes, with Ms. MCCOLLUM in the chair.

The Clerk read the title of the bill.

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

Under the rule, the gentleman from Tennessee (Mr. GORDON) and the gentleman from Texas (Mr. HALL) each will control 30 minutes.

The Chair recognizes the gentleman from Tennessee.

Mr. GORDON of Tennessee. Madam Chairman, I yield myself such time as I may consume.

I would like to begin by thanking my colleagues, Dr. LIPINSKI, Dr. EHLERS, Mr. WU, Mr. SMITH and Mr. HALL for their contributions to the good bipartisan bill we are considering today. I would also like to take a moment to thank the various staffers who worked on this bill: Marcy Gallo, Travis Hite, Dahlia Sokolov and Mike Quear on the majority side; and Dan Byers and Mele Williams on the minority staff. We could not bring a good bill like this together without their help.

Last fall, the House passed a resolution recognizing National Cybersecurity Awareness Month. The resolution stated that we will need to build strong partnerships between Federal agencies, business and nongovernmental organizations and educational institutions in order to enhance the state of cybersecurity in the United States.

H.R. 4061 implements this principle of public-private partnerships in three areas: coordinating and prioritizing the Federal cybersecurity R&D portfolio, improving the transfer of cybersecurity technologies to the marketplace, and training an IT workforce that can meet the growing needs of both public and private sectors.

H.R. 4061 strengthens research and innovation partnerships through the requirement for a strategic plan for cybersecurity R&D that is based on an assessment of risk to our Nation and its population. In developing this plan, the Federal Government must solicit input from all stakeholders, including industry and colleges and universities. The plan must also describe how the agencies will support the transfer of promising technologies from our national labs and universities to the private sector.

Finally, the Federal agencies must convene a university-industry task force to explore collaborative models of cybersecurity. We need to get the best ideas of our scientists and engineers out of the lab and into the marketplace where they can contribute to our collective security and general economic growth.

H.R. 4061 builds educational partnerships to create a well-trained workforce and an informed public. Specifically, H.R. 4061 taps into our colleges and universities by providing scholarships to students pursuing degrees in cybersecurity in exchange for their service in the Federal IT workforce. The legislation also requires NIST to disseminate the cybersecurity best practices to individuals and small businesses in a more user-friendly format.

But the Internet doesn't stop at our borders, which means that improving cybersecurity also requires international partnerships. H.R. 4061 addresses this by requiring NIST to develop a comprehensive international cybersecurity strategy that defines what cybersecurity technical standards we need, where they are being developed, and ensures that the United States is represented.

Many organizations support this legislation, including the U.S. Chamber of Commerce, U.S. Telecommunication Association, the National Cable and Telecommunications Association, the Business Software Alliance, the Association for Computing Machinery, the Computing Research Association, Sun Micro Systems, the University of Illinois at Urbana, the Georgia Institute of Technology, the Software and Information Industry Association, Applied Visions, Inc., Verisign, CA, Inc., Symantec Corporation, McAfee, Inc., and TechAmerica, among others.

But we have also had the support of our colleagues from New York and the chairman of the Oversight and Government Reform Committee, Mr. TOWNS. And at this point, I would like to insert an exchange of letters into the RECORD between myself and Mr. TOWNS.

HOUSE OF REPRESENTATIVES, COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, DC, February 2, 2010.

Hon. BART GORDON,
Chairman, Committee on Science and Technology, Rayburn House Office Building, Washington, DC.

DEAR CHAIRMAN GORDON: I write to you regarding H.R. 4061, the ''Cybersecurity Enhancement Act of 2009''.

H.R. 4061 contains provisions that fall within the jurisdiction of the Committee on Oversight and Government Reform, including provisions related to the federal workforce. I recognize and appreciate your desire to bring this legislation before the House in an expeditious manner and, accordingly, I will not seek a sequential referral of the bill.

However, agreeing to waive consideration of this bill should not be construed as the Committee on Oversight and Government Reform waiving its jurisdiction over H.R. 4061. Further, the Committee on Oversight and Government Reform reserves the right to seek the appointment of conferees during any House-Senate conference convened on this legislation on provisions of the bill that are within the Committee's jurisdiction.

I look forward to working with you as we prepare to pass this important legislation.

Sincerely,

EDOLPHUS TOWNS,
Chairman.

HOUSE OF REPRESENTATIVES, COMMITTEE ON SCIENCE AND TECHNOLOGY,
Washington, DC, February 2, 2010.

Hon. EDOLPHUS TOWNS,
Chairman, Committee on Oversight and Government Reform, House of Representatives, Rayburn House Office Building, Washington, DC.

DEAR CHAIRMAN TOWNS: Thank you for your February 2, 2010 letter regarding H.R. 4061, the Cybersecurity Enhancement Act of 2009. Your support for this legislation and your assistance in ensuring its timely consideration are greatly appreciated.

I agree that provisions in the bill are of jurisdictional interest to the Committee on Oversight and Government Reform. I acknowledge that by forgoing a sequential referral, your Committee is not relinquishing its jurisdiction and I will fully support your request to be represented in a House-Senate conference on those provisions over which the Committee on Oversight and Government Reform has jurisdiction in H.R. 4061. A copy of our letters will be placed in the Congressional Record during consideration of the bill on the House floor.

I value your cooperation and look forward to working with you as we move ahead with this important legislation.

Sincerely,

BART GORDON,
Chairman.

In conclusion, H.R. 4061 is a good, bipartisan bill that strengthens public-private partnerships, ensures an overall vision for the Federal cybersecurity R&D portfolio, trains the next generation of cybersecurity professionals, and improves the cybersecurity technical standards.

I urge my colleagues to support H.R. 4061.

Madam Chair, I reserve the balance of my time.

Mr. HALL of Texas. Madam Chairman, I yield myself such time as I may consume.

I rise in support of H.R. 4061. We are all aware of the importance of cybersecurity and how it has grown dramatically in recent years, as most of the critical systems upon which we depend, from telecommunications to electricity to banking and commerce, rely on secure and reliable computing.

□ 1300

There are short-term policy actions that we can and must take to protect our networks, but over the long term the key to cybersecurity is winning the technological race against our adversaries. That is what this legislation is really aimed toward.

The Science and Technology Committee has a long record of leadership on these issues, dating back to the 1980s, led well by the gentleman from Tennessee, and the agencies and programs we oversee are critical to the success of Federal efforts to address cybersecurity weaknesses and their threats.

This bill will help to support these efforts through authorization of activities in three general areas: the first one being basic research at the National Science Foundation; the second one, expanded NSF scholarships to increase the size and skills of the cybersecurity workforce; and third, increase R&D standards, development and coordination, and public outreach at the National Institute of Standards and Technology related to cybersecurity.

Now, these are modest but important changes that will help us do a better job of protecting our communications network, and I am pleased to join my fellow Texan, Mr. MCCAUL, as a cosponsor, along with two of our key subcommittee ranking members, Dr. EHLERS of Michigan and Representative SMITH of Nebraska.

I also want to note my appreciation for what this bill doesn't do. It avoids calling for any activities that could amount to being regulatory in nature. I think this is important. The committee heard from multiple outside witnesses that heavy Federal involvement in private sector cybersecurity processes would actually be counterproductive to security. I hope we can ensure this bill continues to restrain from such action as it moves through the legislative process.

This is a good bill, and it represents a small but important step in the government's overall efforts to address cybersecurity issues. I want to thank Chairman GORDON and our colleagues in the majority for working closely with the Republicans on this legislation, and I look forward to continued cooperative efforts as we move forward.

I reserve the balance of my time.

Mr. GORDON of Tennessee. Madam Chair, I yield 5 minutes to the gentleman from Illinois, the primary sponsor of this good bipartisan bill, Dr. LIPINSKI, who has just gotten back from home and a 78 percent victory in his primary last night. Congratulations.

Mr. LIPINSKI. Madam Chair, I would like to begin by thanking Chairman GORDON for all his work on this bill and on the cybersecurity issue in general. This is, as the chairman said, a good bipartisan bill. I also want to thank Ranking Member HALL for his work and Dr. EHLERS, as we worked on the Research and Science Education Subcommittee on this bill.

Almost a year ago, President Obama called for a comprehensive 60-day review of U.S. cyberspace policy. This call and the expert recommendations contained in the resulting report led to a series of hearings in my Research and Science Education Subcommittee as well as the full Science and Technology Committee. We heard in these hearings about the various aspects of cybersecurity R&D, including the state of research programs, partnerships with the private sector, the IT workforce, and how both NIST and the NSF are responding to the review.

H.R. 4061 is built upon what we learned in these hearings and addresses some of the critical issues raised in the 60-day review. Specifically, it aims to build strong public-private partnerships, improve the transfer of cybersecurity technologies to the marketplace, train an IT workforce for both the public and private sectors, and coordinate and prioritize Federal cybersecurity R&D.

Information technology is an integral part of all of our daily lives. Computers, cell phones, and Internet have greatly increased our productivity and connectivity. Unfortunately, this connectivity and dependence of our critical infrastructure on information technology have increased our vulnerability to cyberattacks. One month ago, we saw a coordinated foreign attack on Google's Web site. Last week, we also saw an infiltration on our House Web site. Last year, the Pentagon reported more than 360 million attempts to break into its network.

But it is not just the Pentagon or House of Representatives that needs to worry about cybersecurity. Cybercrime is a problem for businesses, large and small, and for every single American. The FTC estimates that identity theft costs consumers about $50 billion annually, and that, even more alarmingly, it is the fastest growing type of fraud in the United States. And these aren't just individual criminals. Increasing globalization in the Internet means that sophisticated organized groups can mine information, selling it both nationally and internationally.

Improving the security of cyberspace is of the utmost importance and will take the collective effort of the Federal Government, the private sector, our scientists and engineers, and every American to succeed, and this bill takes an important step forward in doing this.

Last fall, as Chairman GORDON said, under the leadership of Congresswoman CLARKE, we passed a resolution recognizing National Cybersecurity Awareness Month. Among other things, this resolution contributed to an important education and awareness campaign, a national effort to make people aware of the problem and to make them think about what I like to call practicing good computer hygiene. However, Federal leadership is not only needed to increase public awareness, but also in research, education and in demonstrating how to secure our systems.

Chairman GORDON gave a very good summary of what is in this bill. I want to focus on one particular aspect a little bit, on education. By that, I mean educating individuals, educating companies, and educating the next generation of IT professionals. H.R. 4061 addresses this by building on existing partnerships, such as the NSF-sponsored Center for Systems Security and Information Assurance at Moraine Valley Community College in Palos Hills, Illinois, in my district. This single school in my district has trained more than 600 cybersecurity faculty since 2003. Individuals are now teaching at community colleges and technical training programs nationwide.

In order to realize the full benefits of information technology, we not only need a highly skilled IT workforce, but also advances in basic R&D. Cyberthreats are constantly evolving, and cybersecurity R&D must evolve in concert through a combination of near-term fixes and long-term projects that build a more secure foundation. And because people are perhaps the weakest link in many IT systems, our research strategies need to include the social and behavioral sciences that can help us better understand how humans interact with technology. This is something that is often overlooked but is contained in this bill.

So, in closing, I just again want to thank Chairman GORDON for his work on this. I am very proud to be the author of this bill, and I urge its passage by the full House.

The CHAIR. The gentleman from Texas is recognized.

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

I rise in support of this bill. I want to thank Ranking Member HALL and I want to thank my good friends across the other side of the aisle, Chairman GORDON and Mr. LIPINSKI, for, as usual, working in a bipartisan way to get good things done for the country. I think the American people deserve that, and they want to see more of that, of us up here in Washington.

I was proud to be the lead Republican sponsor on this bill as well because this issue is so important. A lot of times when you talk about cybersecurity, people's eyes kind of glaze over, and yet when we talk about cybersecurity, we are really talking about national security. We held hearings both in the Science and Technology Committee and on the Homeland Security Committee where we examined the vulnerabilities and the threats presented by cyberattacks, and it is very frightening.

When you talk to the top military advisers to the President, they will tell

you one of the greatest threats we face as a Nation is a cyberattack and that we are vulnerable. And when we had hearings on the issue, we heard that just about every Federal agency, in fact every one, including the Pentagon, had been hacked into and this institution had been hacked into. And there have been major data dumps where information was stolen from countries that we cannot speak of in the well of the floor right now, but foreign countries stealing information from the United States Government.

There are really several areas. There are criminal enterprises who use cyberattacks to steal intellectual property, and then there is the realm of espionage, where we have countries that go in and steal information from the United States Government, intellectual property, secrets within the government, data dumps the size of the Library of Congress. We had a classified program that was subsequently declassified that showed that through the click of a mouse power grids could be blown up.

Every critical infrastructure is tied to cybernetworks. Whether it be our utilities, our power grids, our financial institutions, whether it be air traffic controllers, virtually every sector is tied to the networks, to the Internet, and, therefore, is vulnerable. This bill I think is a good step forward in helping to protect our networks, certainly in the Federal Government.

Last year, I joined with Congressman JIM LANGEVIN from Rhode Island, working with CSIS, who had worked on the Iraq Study Group as well, to put together a team, a commission of experts across the Nation of cyberexperts to make recommendations to the next President of the United States. We made those recommendations to President Obama. I am pleased that this bill actually fulfills one of the main recommendations in that report, and that is to provide improving Federal cyberworkforces within the Federal Government. And this bill does a lot more than that.

Improving research and development, this bill establishes cybersecurity R&D grant programs that focus on technical and human behavioral aspects of cybersecurity. It improves our Federal cyberworkforce. It creates a scholarship program at NSF that can be repaid by Federal service. And, it improves coordination in the government. It gives NIST the authority to set security standards for Federal computer systems and develop checklists for agencies to follow. I think this is a very, very important point, because in our hearings, when we asked the Department of Homeland Security or representatives from the Department of Defense or NSA who is in charge of defending our networks, who is in charge, they couldn't answer that question, because there isn't one person in charge.

One of our recommendations was to have someone at the White House level be put in charge to coordinate the various agencies. And because there is no one in charge, there is the lack of coordination. So the very entities that have the offensive capability for cyberattack are not coordinating with the agencies that are tasked with defending the Nation from a cyberattack. I think that giving NIST the authority to set these standards for the first time is going to go a long way in protecting our networks inside the Federal Government.

It also reaches out to the private sector, which I particularly like about this bill. It emphasizes the implementation of checklists by Federal agencies that they should remain flexible and technology neutral in working with the private sector. It improves coordination outside the government by creating a task force of the Federal Government universities who know this issue very well and the private sector to coordinate the research and development.

I think the idea of a public-private partnership rather than having bureaucrats in Washington make all these decisions is vitally important, to bring in the expertise of the private sector and the technology sector who know this issue very well. And, as Chairman GORDON mentioned, this has broad-based support from business groups outside in the private sector and from the technology sector in particular.

□ 1315

So with that, I think this is a great first step towards protecting our Federal networks. I again want to commend the great leadership on both sides of the aisle for making this happen today.

I reserve the balance of my time.

Mr. GORDON of Tennessee. First, I want to thank my friend from Texas for both his cosponsorship of this bill, but more importantly, his constructive, productive, bipartisan approach to bringing together this good bill.

I want to now yield 5 minutes to the gentleman from Oregon, primary sponsor of the bill, the chairman of our Technology and Innovation Subcommittee, Mr. WU.

Mr. WU. Madam Chair, I rise today in strong support of H.R. 4061, which will improve our Nation's cybersecurity by supporting research, create usable technical standards, and promote cybersecurity education. Cybersecurity is critically important, and I want to commend our chairman, Chairman GORDON, for bringing this legislation to the floor today and for his long term leadership on this issue.

The recent cyber attack perpetrated by China against Google and numerous other American companies is a stark reminder of the vulnerabilities we face in an electronically interconnected world. More and more of our personal information is making its way online. Everything from traffic control systems and air traffic control to manufacturing and banking depends on Internet networked systems.

Within the Science Committee, the Technology and Innovation Subcommittee, which I chair, has been exploring ways that the National Institute of Standards and Technology's expertise in information technology can be used to advance the administration's goal of securing cyberspace. Twenty-two years ago the Science and Technology Committee paved the way for Federal cybersecurity efforts with the Computer Security Act of 1987, the first of 13 major laws related to cybersecurity. The 1987 bill charged NIST with developing technical standards to protect nonclassified information in Federal computer systems.

H.R. 4061 improves on these ongoing efforts by implementing recommendations made in the Cyberspace Policy Review and in a hearing my subcommittee held last October. The Cyberspace Policy Review and witnesses at our hearing stressed the importance of increased coordination as the Federal Government works on international technical standards, an education awareness campaign for all Internet users, and improved identity management systems. NIST has a leadership role to play in all three of these critical areas.

The U.S. Government must better coordinate its efforts to develop international cybersecurity technical standards. These responsibilities are currently divided among numerous agencies without any coordinated, consistent policy. A coordinated, consistent policy will ensure U.S. representatives operate with the overarching needs of our Nation in mind when they negotiate.

Witnesses testified before the Technology and Innovation Subcommittee that NIST is suited for the role of policy coordinator because of extensive technical expertise, established relationships with international bodies, and the fact that it is a nonregulatory body. Experts also called for a cybersecurity awareness and education campaign.

While NIST can be a valuable resource for Internet users by providing consumers with the same guidance it gives to Federal agencies, witnesses have noted that NIST guidance is often too technical for the average Internet user. The legislation before us today tasks NIST with developing a plan to make its standards and best practices usable by those with less technical expertise.

In simple terms, 70, 80, 90 percent of needed cybersecurity improvement can be achieved by using available methods and technology. Take simple steps. Do back up your data. Don't back up data and take it home in an open, unlocked car. It is like clicking your seatbelt before you drive or washing hands before a surgeon operates on a patient. Commonsense steps, available methods and technology; simply put, good computer hygiene.

We also know that cybersecurity cannot be improved without first improving identity management. Today's bill

builds upon NIST's ongoing work on identity management systems, such as biometrics, by tasking NIST with improving the interoperability of these systems to encourage more widespread use. By focusing on the usability and privacy aspects of identity management, this bill will encourage greater confidence in the general public that their personal information will be secure.

Madam Chair, securing cyberspace is a primary concern of each and every one of us. We cannot stand by and let the most powerful tool for connecting Americans with each other and the world remain a technologic wild west. It is time to fence the prairie to make it available to the technologic communities of the future.

I urge my colleagues to join me in supporting H.R. 4061 so that our communities and our constituents can be secure in the knowledge that they are safe when they go online.

Mr. MCCAUL. I yield as much time as he may consume to the gentleman from Georgia (Mr. KINGSTON).

Mr. KINGSTON. I thank the gentleman for yielding.

Madam Chairman, when I first came to Congress in 1993, we had computers but we did not have Internet. In fact, if it wasn't for Al Gore maybe we still wouldn't have it. I don't need to bring that up.

But you know, the reality is most of us, and my friend Mr. GORDON will remember, did not have cell phones. And then I remember there was a discussion that I had with one Member about, ''You know, I don't think it is fair for the taxpayers to pay for your cell phone. I think it is unnecessary.''

And I remember when I got a cell phone I wanted to have a 912 area code, because I didn't want the folks back home to think I went Washington if I had the 202 area code. But now in essence everybody has a mobile phone, as they do Internet. I remember Stacy Hall, our receptionist, who was the IT person since she was the youngest in the office. She was probably 22, a UGA graduate. She got this thing called the Internet, and she started planning her weekends with her friends.

Now, there were about five other 21-, 22-year-old kids on the Hill who knew what email was. So they started swapping. And then I remember eventually she told our scheduler about, ''You know, maybe you could use this like to schedule the Congressman.'' What a radical idea. And before you know it, 5 or 6 years down the road, everybody was addicted to it.

And then I remember 9/11, not many of us had a BlackBerry. But BlackBerrys had an ability to get out on the Internet a little bit better than cell phones, so BlackBerrys became an important thing. And I know Mr. GORDON and many of us here have seen all this grow, but now this phenomenal piece of equipment can find maps anywhere in the world. You can talk to somebody on the phone. You can take pictures and instantly send it to somebody. You can download music—although I have no idea how—and Internet people and look up things, Google online and Bing. And can you only imagine what this will be 5 years from now. It is unbelievable.

I entered Michigan State University, and the calculator was a slide rule. We actually voted my freshman year not to allow calculators because the Texas Instruments, I think it was called an SR–10—can I get an amen over there? I know you must have had one. It was $179. We voted in my chemistry class at Michigan State University not to allow calculators because most middle class kids could not afford it. And yet 4 or 5 years later you could get much better calculators that fit in your pocket for $10.

Technology has evolved at such a rapid pace, and yet along with it so have the bad guys. It used to be that maybe some interested math genius with a twisted sense of humor in Indonesia would hack into the Department of Defense computers just to see if he could, not really caring how many F–22s were in production, but just wanted to know. But then eventually the bad guys became more organized, more sophisticated, botnets, computer systems that talked to each other and shared information. A way of hacking into the Department of Defense, the Department of Energy, the Centers for Disease Control, all kinds of government agencies with all kinds of sensitive information. But there is no need to stop there. Wall Street, financial information, other things that you could get out of universities, all of it is vulnerable.

And so this bill today is relevant because it shows that Congress is moving along with the technology to rise to the challenge. We need to have cybersecurity experts. So many of the cybersecurity experts that we have now come up through a law enforcement background and then they learn their computer training.

What this bill does is to reach out to that young 17-, 18-, 19-year-old, and identify them as being interested in this, and merge in all their talents and say come on in the classroom because we need you as a line of defense. Technology against technology has to have that wall in-between them, and that wall is a brilliant, well-trained human being. That is what this bill seeks to do.

In my own district, I have to brag a little bit, that Armstrong Atlantic University has a Cyber Security Research Institute. And it is working to bridge the gap so that the young people can have a viable career in cybersecurity. The program is to produce a more educated cybersecurity investigator with expertise in areas not only in technology but in law enforcement and law itself, and policy itself, and work with cyber forensics in order to produce the kind of professionals that we need to overcome the threat that we face as a Nation. We cannot be passive about this topic. We have to be proactive.

This bill shows one of the great bipartisan efforts of Congress, for us to come together and address something that is truly a national security threat. So I am proud to support it. If you want any more information, you can get it on my BlackBerry. I will be glad to download it for you.

Mr. GORDON of Tennessee. Madam Chairman, I want to thank my friend from Savannah for the history lesson there, and let him know that my 8-year-old daughter can be some help to him if he wants to download any of his music.

Mr. KINGSTON. If the gentleman would yield?

Mr. GORDON of Tennessee. She can help me, too.

Mr. KINGSTON. Especially if it is some of that good Tennessee music that you all produce.

Mr. GORDON of Tennessee. Madam Chairman, I yield 2½ minutes to the gentleman from Maryland (Mr. RUPPERSBERGER), a member of the important Intelligence Committee.

Mr. RUPPERSBERGER. Madam Chair, I rise in support of H.R. 4061, the Cybersecurity Enhancement Act.

I want to thank Chairman GORDON, Congressman WU, Ranking Member HALL, and Congressman MCCAUL for your bipartisan effort. You know, this is truly an example of working together on behalf of our citizens. If we could only do this on other issues such as health care and whatever, we would be a lot better off as a country. So thank you for your leadership, and let's continue this bipartisanship effort.

Cyber networks power almost everything we do, from our computers and cell phones and iPods to the electrical grid that allows us to turn on our lights. They also operate the classified military and intelligence networks that keep us safe and provide critical data to our troops in combat.

As a member of the Intelligence Committee and chairman of the Technical and Tactical Subcommittee, which oversees the technical aspects of cybersecurity, I know that protecting our cyber networks is a top economic and national security priority. We are under attack each and every day. These attacks have cost the U.S.A. $1 trillion last year, and also put classified information in the hands of our enemies.

Cybersecurity is a tough challenge because the government does not own the Internet. In fact, 85 percent of cyber is held privately. We have to get the public and private sectors on the same page, and this bill does that. This bill directs the National Institute of Standards and Technology, the measurement laboratory for our Nation, based in Maryland, to develop international cybersecurity technical standards. It also charges NIST with creating education campaigns for the public, a critical component to meeting this challenge.

This bill also helps to ensure that we have the workforce in place to meet the new demands by providing scholarships to students who agree to work as cybersecurity specialists after graduation. The bill also funds faculty and curriculum development at U.S. colleges and universities to help with the shortage of qualified cyber professors.

□ 1330

I also support the amendment proposed by my Maryland colleague, Congressman KRATOVIL, to establish a National Center of Excellence for Cybersecurity to consolidate our resources into one cyberclearinghouse. Protecting our Nation's network is not a Democratic or Republican initiative; it is USA first.

The CHAIR. The time of the gentleman has expired.

Mr. GORDON of Tennessee. I yield the gentleman 20 additional seconds.

Mr. RUPPERSBERGER. Let's pass H.R. 4061 and make sure our own cybernetworks don't become a new weapon in our enemies' arsenals.

Mr. MCCAUL. I reserve the balance of my time.

Mr. GORDON of Tennessee. Madam Chairman, I yield 2 minutes to the co-chair of the House Cybersecurity Caucus, the gentleman from Rhode Island (Mr. LANGEVIN).

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

Mr. LANGEVIN. I thank the gentleman for yielding. Madam Chair, I rise today in strong support of the Cybersecurity Enhancement Act of 2009. I'd like to thank Chairman LIPINSKI and also Chairman GORDON for their efforts in bringing this important bill to the floor today.

In today's interconnected world, the American people expect their government's networks to have the same level of access and efficiency as the private sector. Further, building a more transparent and effective government requires leveraging new technologies to strengthen coordination between our Federal agencies, in addition to strengthening our communications with the citizens of our Nation. To achieve these goals, it is absolutely critical that our Federal networks and information systems are safe and secure.

Despite increased attention in recent years by the Congress and the administration on cybersecurity, our Federal networks remain exceptionally vulnerable still to attack. Securing them will require increased emphasis on coordination and technological advancements. I, of course, understand that the NSA and the very talented, dedicated workforce that work on cyberissues are the best in the world at what they do, but it will also require the United States to strengthen domestic cybersecurity talent and find new ways to leverage the expertise that exists in the private sector. This will be a true force multiplier for us. This bill takes significant steps toward achieving those goals by strengthening Federal cybersecurity standards, increasing research and development, and evaluating how to improve our Federal cybersecurity workforce.

That being said, we as a Nation cannot afford to fail in these efforts, and I urge my colleagues to join me in supporting this very important piece of legislation.

Mr. MCCAUL. Just in closing, I co-chair the Cybersecurity Caucus with Congressman LANGEVIN, and I want to commend him for his great work not only on the CSIS Commission but also on the caucus to try to raise awareness of this issue. It is a very, very important issue. I also want to thank Chairman GORDON, who I know is going to retire. We're going to miss him. But just the bipartisan spirit in which he has conducted himself on this committee to allow us to work together with the majority to get good legislation out of the Congress. As I said earlier, I think that's what the American people want. It's what they deserve. Certainly, there's no greater issue where Republicans and Democrats should come together than on issues impacting national security, which this bill does. We are Americans first. Again, this bill is a great step forward into furthering and protecting our Federal networks.

I hope, as with what happened with 9/11, we don't turn a blind eye and wait until there's a major denial of service attack before we start to pay attention to this issue. I think this bill, which I anticipate will pass the House overwhelmingly, is a great statement by the Congress that cybersecurity is important and that we can work together on this. I think, as Congressman WU talked about the attacks on Google recently, last Fourth of July we had a denial of service attack emanating that hit Korea and the United States. The disturbing thing about that attack was it was not to phish or to steal information, or perhaps espionage. Rather, it was intended to do harm. That denial of service attack was intended to shut down our networks. It was relatively unsophisticated.

But as we examine the denial of service attacks that we saw in Estonia, the denial of service attack in Korea and the United States just last Fourth of July, to me, that is an eye opener. It's just like before 9/11 we saw signs that the Congress needed to pay attention to. I think we have seen signs of that in the cyber-realm, and I hope we can work together across the aisle to further enhance and strengthen our cybernetworks, and in the private sector as well, so that we can avoid a cyber-9/11 attack in the United States.

So this is, again, a very important issue that, when you talk to leaders in the military, they get it. They recognize it. They want to work with the Congress to better improve our cybersecurity. Again, let me just give my thanks to Chairman GORDON for allowing this to come out of the committee and come to the House floor. I urge my colleagues on both sides of the aisle to support this legislation.

I yield back the balance of my time.

Mr. GORDON of Tennessee. In closing, let me just suggest to my friend from Texas that bipartisanship goes both ways, and I want to thank him for his great input in this bill, as well as Dr. EHLERS, Mr. HALL, Mr. WU, and Dr. LIPINSKI. It was a good team effort. And certainly our staffs were integral to having this be a successful bill. I agree with you—hopefully this will pass overwhelmingly and will send a message to the bad guys that we're on alert.

Mr. GOODLATTE. Madam Chair, I rise in support of H.R. 4061.

Recent attacks on Government networks have served to increase awareness that cybersecurity is not just about protecting computers, but also has implications for U.S. national security and economic well-being. Without confidence in our Nation's internet infrastructure and data security, I am concerned that our country will not be able to climb out of the current economic climate. As such, I was pleased when President Obama declared in a speech in May 2009 that U.S. critical information infrastructures are a ''Strategic National Asset''.

Unfortunately, since that speech, the Administration's actions have not been indicative of those necessary to protect such a ''Strategic National Asset.'' While I appreciate that the President recently appointed Howard Schmidt as Cyber Coordinator, this appointment was long overdue.

Madam Chair, A recent GAO report stated that, ''Pervasive and sustained cyber attacks continue to pose a potentially devastating threat to the systems and operations of the Federal Government.'' The report went on to further state that, ''The ever-increasing dependence of Federal agencies on computerized systems to carry out essential, everyday operations can make them vulnerable to an array of cyber-based risks. Thus it is increasingly important for the Federal Government to have effective information security controls in place to safeguard its systems and the information they contain.''

In response to this GAO report and extensive hearings by the House Science and Technology Committee, I am pleased to support the Committee's bi-partisan legislation and applaud its authors. Specifically, H.R. 4061 authorizes activities in three areas in support of increased Federal focus on cybersecurity. This legislation:

Continues support of basic research at the National Science Foundation (NSF);

Expands NSF scholarships to increase the size and skills of the cybersecurity workforce; and

Increases R&D, standards development and coordination, and public outreach at the National Institute of Standards and Technology (NIST) related to cybersecurity.

I also appreciate that this bill is not too overly burdensome and shies away from an overly regulatory approach. H.R. 4061 is a good first step as the 111th Congress addresses cybersecurity and I look forward to continuing this dialogue. I ask my colleagues to join me in support of H.R. 4061.

Ms. JACKSON LEE of Texas. Madam Chair, I rise today in support of H.R. 4061, ''The Cybersecurity Enhancement Act of 2009,'' and I would like to thank my colleagues Representative LIPINSKI for introducing this measure, and Representative EHLERS, Representative WU, Representative SMITH and Representative HALL for their contributions to gain bipartisan support on this very important legislation that we are considering today.

This bill will help ensure a strategic plan for Federal Cybersecurity Research & Development (R&D) activities, strengthen public-private partnerships in cybersecurity, help train the next generation of cybersecurity professionals, and improve cybersecurity technical standards.

As we may recall, almost a year ago President Obama called for a comprehensive 60 day review of U.S. cyberspace policy. This review and the recommendations contained in the report led to a series of hearings on various aspects of cybersecurity R&D, including the state of research programs, partnerships with the private sector, the IT workforce, and how both NIST and the NSF are responding to the review.

H.R. 4061 is built upon these hearings, and addresses the issues raised in the 60-day review. Specifically, it aims to build strong public-private partnerships, improve the transfer of cybersecurity technologies to the marketplace, train an IT workforce for both the public and private sectors, and coordinate and prioritize Federal cybersecurity R&D. Of course cybersecurity research, standards setting, and education are only one piece of the recommendations of the 60-day report, and are only part of the solution. However, it is the beginning to a wide spread need to improving the security of cyberspace is that is one of the utmost importance and it will take the collective effort of the Federal Government, the private sector, our scientists and engineers, and every American to succeed.

Our Nation's cyber-infrastructure is an interconnected combination of private, public and Government networks. It is critical that Government and industry work closely to protect both the infrastructure and the future of innovation. Giving them the tools to ensure they can protect themselves—access to timely action-oriented information and availability of insurance for cyber incidents—as well as encouraging critical cybersecurity R&D here in the U.S., are the most important efforts our Administration can take to secure our cyber-infrastructure.

While we have been fortunate so far in avoiding a catastrophic cyber attack, last year the Pentagon reported more than 360 million attempts to break into its networks. A 2009 Consumer Reports study found that over the past two years, one in five online consumers has been a victim of cyber crime. In 2008 the Department of Homeland Security logged 5,499 such cyber attack incidents—a 40 percent increase over the previous year. A 2007 Government Accountability Office report estimates the total U.S. business losses due to cyber attacks exceed $117.5 billion per year.

I urge your support of this bill for we are all aware of the growing number of internet security incidents, involving such things as computer viruses, denial of service attacks, and defaced Web sites. These events have disrupted business and government activities, and have sometimes resulted in significant recovery costs.

It is important that we take inventory of all systems that are vital to the functioning of the Nation, and do all we can to protect them. This certainly includes our computer networks systems that can be attacked anonymously and from far away. These networks are the glue that holds our Nation's infrastructure together. An attack from cyberspace could jeopardize electric power grids, railways, hospitals and financial services, to name a few.

Last fall, under the leadership of Congresswoman CLARKE, we passed a resolution recognizing National Cybersecurity Awareness Month. Among other things this resolution contributed to an important education and awareness campaign, a national effort to make people aware of the problem. However, Federal leadership not only needed to increase public awareness, but also in research, education, and in demonstrating how to secure our own systems. Again, H.R. 4061 ensures an overall vision for the Federal cybersecurity R&D portfolio, trains the next generation of cybersecurity professionals, and improves cybersecurity technical standards.

It is now time for a broad-reaching, forward-thinking approach and the successful passage of H.R. 4061 is the beginning to bridge the gap and collaborate and coordinate with the private sector to conquer the many challenges to improve our country's security through cybersecurity.

As a member of the Homeland Security Committee, I am committed to working with my colleagues, businesses, and educational institutions to enhance the development and implementation of existing and future cyber security standards that enhance the Nation's security. Madam Chair, I support H.R. 4061.

Ms. EDDIE BERNICE JOHNSON of Texas. Madam Chair, today I rise in support of the Cyber Security Enhancement Act of 2009. Nearly 1 year ago, the administration called for a 60-day review of the national cyber security strategy. The report found that our Nation's digital infrastructure was largely at risk to a growing threat of cybercrime. Major advances in cyber security research and development were needed to address the report's findings. In order to protect against these sorts of intrusions I, along with other Members on the House Science and Technology Committee, worked to draft legislation that would address these findings.

During the Research and Science Education subcommittee markup on September 23, 2009, I amended this legislation to include a description of how the program will help contribute to a more diverse workforce by including women and minorities. This can be achieved by partnering Minority Serving Institutions, in addition to stakeholders in industry, academia, and other relevant organizations. Promoting broader participation of women and underrepresented minorities will only benefit the intent of this legislation.

I urge the passage of the Cyber Security Enhancement Act of 2009 which addresses many of the concerns in the administration's review. By adopting a comprehensive national cyber security research and development plan we will drastically advance American innovation in cyber security. I am proud to have worked towards securing some of America's vulnerabilities in cyberspace while increasing public education in this area of technology.

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

The CHAIR. All time for general debate has expired.

Pursuant to the rule, the amendment in the nature of a substitute printed in the bill shall be considered as an original bill for the purpose of amendment under the 5-minute rule and shall be considered read.

The text of the committee amendment is as follows:

H.R. 4061

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

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Cybersecurity Enhancement Act of 2009''.

TITLE I—RESEARCH AND DEVELOPMENT

SEC. 101. DEFINITIONS.

In this title:

(1) NATIONAL COORDINATION OFFICE.—The term National Coordination Office means the National Coordination Office for the Networking and Information Technology Research and Development program.

(2) PROGRAM.—The term Program means the Networking and Information Technology Research and Development program which has been established under section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511).

SEC. 102. FINDINGS.

Section 2 of the Cyber Security Research and Development Act (15 U.S.C. 7401) is amended—

(1) by amending paragraph (1) to read as follows:

''(1) Advancements in information and communications technology have resulted in a globally interconnected network of government, commercial, scientific, and education infrastructures, including critical infrastructures for electric power, natural gas and petroleum production and distribution, telecommunications, transportation, water supply, banking and finance, and emergency and government services.'';

(2) in paragraph (2), by striking ''Exponential increases in interconnectivity have facilitated enhanced communications, economic growth,'' and inserting ''These advancements have significantly contributed to the growth of the United States economy'';

(3) by amending paragraph (3) to read as follows:

''(3) The Cyberspace Policy Review published by the President in May, 2009, concluded that our information technology and communications infrastructure is vulnerable and has 'suffered intrusions that have allowed criminals to steal hundreds of millions of dollars and nation-states and other entities to steal intellectual property and sensitive military information'.'';

(4) by redesignating paragraphs (4) through (6) as paragraphs (5) through (7), respectively;

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

''(4) In a series of hearings held before Congress in 2009, experts testified that the Federal cybersecurity research and development portfolio was too focused on short-term, incremental research and that it lacked the prioritization and coordination necessary to address the long-term challenge of ensuring a secure and reliable information technology and communications infrastructure.''; and

(6) by amending paragraph (7), as so redesignated by paragraph (4) of this section, to read as follows:

''(7) While African-Americans, Hispanics, and Native Americans constitute 33 percent of the college-age population, members of these minorities comprise less than 20 percent of bachelor degree recipients in the field of computer sciences.''.

SEC. 103. CYBERSECURITY STRATEGIC RESEARCH AND DEVELOPMENT PLAN.

(a) IN GENERAL.—Not later than 12 months after the date of enactment of this Act, the agencies identified in subsection 101(a)(3)(B)(i) through (x) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(3)(B)(i) through (x)) or designated under section 101(a)(3)(B)(xi) of such Act, working through the National Science and Technology Council and with the assistance of the National Coordination Office, shall transmit to Congress a strategic plan based on an assessment of cybersecurity risk to guide the overall direction of Federal cybersecurity and information assurance research and development for information technology and networking systems. Once every 3 years after the initial strategic plan is transmitted to Congress under this section, such agencies shall prepare and transmit to Congress an update of such plan.

(b) CONTENTS OF PLAN.—The strategic plan required under subsection (a) shall—

(1) specify and prioritize near-term, mid-term and long-term research objectives, including objectives associated with the research areas identified in section 4(a)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(1)) and how the near-term objectives complement research and development areas in which the private sector is actively engaged;

(2) describe how the Program will focus on innovative, transformational technologies with the potential to enhance the security, reliability, resilience, and trustworthiness of the digital infrastructure;

(3) describe how the Program will foster the transfer of research and development results into new cybersecurity technologies and applications for the benefit of society and the national interest, including through the dissemination of best practices and other outreach activities;

(4) describe how the Program will establish and maintain a national research infrastructure for creating, testing, and evaluating the next generation of secure networking and information technology systems;

(5) describe how the Program will facilitate access by academic researchers to the infrastructure described in paragraph (4), as well as to relevant data, including event data; and

(6) describe how the Program will engage females and individuals identified in section 33 or 34 of the Science and Engineering Equal Opportunities Act (42 U.S.C. 1885a or 1885b) to foster a more diverse workforce in this area.

(c) DEVELOPMENT OF ROADMAP.—The agencies described in subsection (a) shall develop and annually update an implementation roadmap for the strategic plan required in this section. Such roadmap shall—

(1) specify the role of each Federal agency in carrying out or sponsoring research and development to meet the research objectives of the strategic plan, including a description of how progress toward the research objectives will be evaluated;

(2) specify the funding allocated to each major research objective of the strategic plan and the source of funding by agency for the current fiscal year; and

(3) estimate the funding required for each major research objective of the strategic plan for the following 3 fiscal years.

(d) RECOMMENDATIONS.—In developing and updating the strategic plan under subsection (a), the agencies involved shall solicit recommendations and advice from—

(1) the advisory committee established under section 101(b)(1) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(b)(1)); and

(2) a wide range of stakeholders, including industry, academia, including representatives of minority serving institutions, and other relevant organizations and institutions.

(e) APPENDING TO REPORT.—The implementation roadmap required under subsection (c), and its annual updates, shall be appended to the report required under section 101(a)(2)(D) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(2)(D)).

SEC. 104. SOCIAL AND BEHAVIORAL RESEARCH IN CYBERSECURITY.

Section 4(a)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(1)) is amended—

(1) by inserting ''and usability'' after ''to the structure'';

(2) in subparagraph (H), by striking ''and'' after the semicolon;

(3) in subparagraph (I), by striking the period at the end and inserting ''; and''; and

(4) by adding at the end the following new subparagraph:

''(J) social and behavioral factors, including human-computer interactions, usability, user motivations, and organizational cultures.''.

SEC. 105. NATIONAL SCIENCE FOUNDATION CYBERSECURITY RESEARCH AND DEVELOPMENT PROGRAMS.

(a) COMPUTER AND NETWORK SECURITY RESEARCH AREAS.—Section 4(a)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(1)) is amended in subparagraph (A) by inserting ''identity management,'' after ''cryptography,''.

(b) COMPUTER AND NETWORK SECURITY RESEARCH GRANTS.—Section 4(a)(3) of such Act (15 U.S.C. 7403(a)(3)) is amended by striking subparagraphs (A) through (E) and inserting the following new subparagraphs:

''(A) $68,700,000 for fiscal year 2010;

''(B) $73,500,000 for fiscal year 2011;

''(C) $78,600,000 for fiscal year 2012;

''(D) $84,200,000 for fiscal year 2013; and

''(E) $90,000,000 for fiscal year 2014.''.

(c) COMPUTER AND NETWORK SECURITY RESEARCH CENTERS.—Section 4(b) of such Act (15 U.S.C. 7403(b)) is amended—

(1) in paragraph (4)—

(A) in subparagraph (C), by striking ''and'' after the semicolon;

(B) in subparagraph (D), by striking the period and inserting ''; and''; and

(C) by adding at the end the following new subparagraph:

''(E) how the center will partner with government laboratories, for-profit entities, other institutions of higher education, or nonprofit research institutions.''; and

(2) by amending paragraph (7) to read as follows:

''(7) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the National Science Foundation such sums as are necessary to carry out this subsection for each of the fiscal years 2010 through 2014.''.

(d) COMPUTER AND NETWORK SECURITY CAPACITY BUILDING GRANTS.—Section 5(a)(6) of such Act (15 U.S.C. 7404(a)(6)) is amended to read as follows:

''(6) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the National Science Foundation such sums as are necessary to carry out this subsection for each of the fiscal years 2010 through 2014.''.

(e) SCIENTIFIC AND ADVANCED TECHNOLOGY ACT GRANTS.—Section 5(b)(2) of such Act (15 U.S.C. 7404(b)(2)) is amended to read as follows:

''(2) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the National Science Foundation such sums as are necessary to carry out this subsection for each of the fiscal years 2010 through 2014.''.

(f) GRADUATE TRAINEESHIPS IN COMPUTER AND NETWORK SECURITY.—Section 5(c)(7) of such Act (15 U.S.C. 7404(c)(7)) is amended to read as follows:

''(7) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the National Science Foundation such sums as are necessary to carry out this subsection for each of the fiscal years 2010 through 2014.''.

(g) POSTDOCTORAL RESEARCH FELLOWSHIPS IN CYBERSECURITY.—Section 5(e) of such Act (15 U.S.C. 7404(e)) is amended to read as follows:

''(e) POSTDOCTORAL RESEARCH FELLOWSHIPS IN CYBERSECURITY.—

''(1) IN GENERAL.—The Director shall carry out a program to encourage young scientists and engineers to conduct postdoctoral research in the fields of cybersecurity and information assurance, including the research areas described in section 4(a)(1), through the award of competitive, merit-based fellowships.

''(2) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the National Science Foundation such sums as are necessary to carry out this subsection for each of the fiscal years 2010 through 2014.''.

SEC. 106. FEDERAL CYBER SCHOLARSHIP FOR SERVICE PROGRAM.

(a) IN GENERAL.—The Director of the National Science Foundation shall carry out a Scholarship for Service program to recruit and train the next generation of Federal cybersecurity professionals and to increase the capacity of the higher education system to produce an information technology workforce with the skills necessary to enhance the security of the Nation's communications and information infrastructure.

(b) CHARACTERISTICS OF PROGRAM.—The program under this section shall—

(1) provide, through qualified institutions of higher education, scholarships that provide tuition, fees, and a competitive stipend for up to 2 years to students pursing a bachelor's or master's degree and up to 3 years to students pursuing a doctoral degree in a cybersecurity field;

(2) provide the scholarship recipients with summer internship opportunities or other meaningful temporary appointments in the Federal information technology workforce; and

(3) increase the capacity of institutions of higher education throughout all regions of the United States to produce highly qualified cybersecurity professionals, through the award of competitive, merit-reviewed grants that support such activities as—

(A) faculty professional development, including technical, hands-on experiences in the private sector or government, workshops, seminars, conferences, and other professional development opportunities that will result in improved instructional capabilities;

(B) institutional partnerships, including minority serving institutions; and

(C) development of cybersecurity-related courses and curricula.

(c) SCHOLARSHIP REQUIREMENTS.—

(1) ELIGIBILITY.—Scholarships under this section shall be available only to students who—

(A) are citizens or permanent residents of the United States;

(B) are full-time students in an eligible degree program, as determined by the Director, that is focused on computer security or information assurance at an awardee institution; and

(C) accept the terms of a scholarship pursuant to this section.

(2) SELECTION.—Individuals shall be selected to receive scholarships primarily on the basis of academic merit, with consideration given to financial need and to the goal of promoting the participation of individuals identified in section 33 or 34 of the Science and Engineering Equal Opportunities Act (42 U.S.C. 1885a or 1885b).

(3) SERVICE OBLIGATION.—If an individual receives a scholarship under this section, as a condition of receiving such scholarship, the individual upon completion of their degree must serve as a cybersecurity professional within the Federal workforce for a period of time equal to the length of the scholarship. If a scholarship recipient is not offered employment by a Federal agency or a federally funded research and development center, the service requirement can be satisfied at the Director's discretion by—

(A) serving as a cybersecurity professional in a State, local, or tribal government agency; or

(B) teaching cybersecurity courses at an institution of higher education.

(4) CONDITIONS OF SUPPORT.—As a condition of acceptance of a scholarship under this section, a recipient shall agree to provide the

awardee institution with annual verifiable documentation of employment and up-to-date contact information.

(d) FAILURE TO COMPLETE SERVICE OBLIGATION.—

(1) GENERAL RULE.—If an individual who has received a scholarship under this section—

(A) fails to maintain an acceptable level of academic standing in the educational institution in which the individual is enrolled, as determined by the Director;

(B) is dismissed from such educational institution for disciplinary reasons;

(C) withdraws from the program for which the award was made before the completion of such program;

(D) declares that the individual does not intend to fulfill the service obligation under this section; or

(E) fails to fulfill the service obligation of the individual under this section,

such individual shall be liable to the United States as provided in paragraph (3).

(2) MONITORING COMPLIANCE.—As a condition of participating in the program, a qualified institution of higher education receiving a grant under this section shall—

(A) enter into an agreement with the Director of the National Science Foundation to monitor the compliance of scholarship recipients with respect to their service obligation; and

(B) provide to the Director, on an annual basis, post-award employment information required under subsection (c)(4) for scholarship recipients through the completion of their service obligation.

(3) AMOUNT OF REPAYMENT.—

(A) LESS THAN ONE YEAR OF SERVICE.—If a circumstance described in paragraph (1) occurs before the completion of 1 year of a service obligation under this section, the total amount of awards received by the individual under this section shall be repaid or such amount shall be treated as a loan to be repaid in accordance with subparagraph (C).

(B) MORE THAN ONE YEAR OF SERVICE.—If a circumstance described in subparagraph (D) or (E) of paragraph (1) occurs after the completion of 1 year of a service obligation under this section, the total amount of scholarship awards received by the individual under this section, reduced by the ratio of the number of years of service completed divided by the number of years of service required, shall be repaid or such amount shall be treated as a loan to be repaid in accordance with subparagraph (C).

(C) REPAYMENTS.—A loan described in subparagraph (A) or (B) shall be treated as a Federal Direct Unsubsidized Stafford Loan under part D of title IV of the Higher Education Act of 1965 (20 U.S.C. 1087a and following), and shall be subject to repayment, together with interest thereon accruing from the date of the scholarship award, in accordance with terms and conditions specified by the Director (in consultation with the Secretary of Education) in regulations promulgated to carry out this paragraph.

(4) COLLECTION OF REPAYMENT.—

(A) IN GENERAL.—In the event that a scholarship recipient is required to repay the scholarship under this subsection, the institution providing the scholarship shall—

(i) be responsible for determining the repayment amounts and for notifying the recipient and the Director of the amount owed; and

(ii) collect such repayment amount within a period of time as determined under the agreement described in paragraph (2), or the repayment amount shall be treated as a loan in accordance with paragraph (3)(C).

(B) RETURNED TO TREASURY.—Except as provided in subparagraph (C) of this paragraph, any such repayment shall be returned to the Treasury of the United States.

(C) RETAIN PERCENTAGE.—An institution of higher education may retain a percentage of any repayment the institution collects under this paragraph to defray administrative costs associated with the collection. The Director shall establish a single, fixed percentage that will apply to all eligible entities.

(5) EXCEPTIONS.—The Director may provide for the partial or total waiver or suspension of any service or payment obligation by an individual under this section whenever compliance by the individual with the obligation is impossible or would involve extreme hardship to the individual, or if enforcement of such obligation with respect to the individual would be unconscionable.

(e) HIRING AUTHORITY.—For purposes of any law or regulation governing the appointment of individuals in the Federal civil service, upon successful completion of their degree, students receiving a scholarship under this section shall be hired under the authority provided for in section 213.3102(r) of title 5, Code of Federal Regulations, and be exempted from competitive service. Upon fulfillment of the service term, such individuals shall be converted to a competitive service position without competition if the individual meets the requirements for that position.

(f) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to appropriated to the National Science Foundation to carry out this section—

(1) $18,700,000 for fiscal year 2010;
(2) $20,100,000 for fiscal year 2011;
(3) $21,600,000 for fiscal year 2012;
(4) $23,300,000 for fiscal year 2013; and
(5) $25,000,000 for fiscal year 2014.

SEC. 107. CYBERSECURITY WORKFORCE ASSESSMENT.

Not later than 180 days after the date of enactment of this Act the President shall transmit to the Congress a report addressing the cybersecurity workforce needs of the Federal Government. The report shall include—

(1) an examination of the current state of and the projected needs of the Federal cybersecurity workforce, including a comparison of the different agencies and departments, and an analysis of the capacity of such agencies and departments to meet those needs;

(2) an analysis of the sources and availability of cybersecurity talent, a comparison of the skills and expertise sought by the Federal Government and the private sector, and an examination of the current and future capacity of United States institutions of higher education to provide cybersecurity professionals with those skills sought by the Federal Government and the private sector;

(3) an examination of the effectiveness of the National Centers of Academic Excellence in Information Assurance Education, the Centers of Academic Excellence in Research, and the Federal Cyber Scholarship for Service programs in promoting higher education and research in cybersecurity and information assurance and in producing a growing number of professionals with the necessary cybersecurity and information assurance expertise;

(4) an analysis of any barriers to the Federal Government recruiting and hiring cybersecurity talent, including barriers relating to compensation, the hiring process, job classification, and hiring flexibilities; and

(5) recommendations for Federal policies to ensure an adequate, well-trained Federal cybersecurity workforce.

SEC. 108. CYBERSECURITY UNIVERSITY-INDUSTRY TASK FORCE.

(a) ESTABLISHMENT OF UNIVERSITY-INDUSTRY TASK FORCE.—Not later than 180 days after the date of enactment of this Act, the Director of the Office of Science and Technology Policy shall convene a task force to explore mechanisms for carrying out collaborative research and development activities for cybersecurity through a consortium or other appropriate entity with participants from institutions of higher education and industry.

(b) FUNCTIONS.—The task force shall—

(1) develop options for a collaborative model and an organizational structure for such entity under which the joint research and development activities could be planned, managed, and conducted effectively, including mechanisms for the allocation of resources among the participants in such entity for support of such activities;

(2) propose a process for developing a research and development agenda for such entity, including guidelines to ensure an appropriate scope of work focused on nationally significant challenges and requiring collaboration;

(3) define the roles and responsibilities for the participants from institutions of higher education and industry in such entity;

(4) propose guidelines for assigning intellectual property rights and for the transfer of research and development results to the private sector; and

(5) make recommendations for how such entity could be funded from Federal, State, and nongovernmental sources.

(c) COMPOSITION.—In establishing the task force under subsection (a), the Director of the Office of Science and Technology Policy shall appoint an equal number of individuals from institutions of higher education and from industry with knowledge and expertise in cybersecurity.

(d) REPORT.—Not later than 12 months after the date of enactment of this Act, the Director of the Office of Science and Technology Policy shall transmit to the Congress a report describing the findings and recommendations of the task force.

SEC. 109. CYBERSECURITY CHECKLIST DEVELOPMENT AND DISSEMINATION.

Section 8(c) of the Cyber Security Research and Development Act (15 U.S.C. 7406(c)) is amended to read as follows:

''(c) CHECKLISTS FOR GOVERNMENT SYSTEMS.—

''(1) IN GENERAL.—The Director of the National Institute of Standards and Technology shall develop or identify and revise or adapt as necessary, checklists, configuration profiles, and deployment recommendations for products and protocols that minimize the security risks associated with each computer hardware or software system that is, or is likely to become, widely used within the Federal Government.

''(2) PRIORITIES FOR DEVELOPMENT.—The Director of the National Institute of Standards and Technology shall establish priorities for the development of checklists under this subsection. Such priorities may be based on the security risks associated with the use of each system, the number of agencies that use a particular system, the usefulness of the checklist to Federal agencies that are users or potential users of the system, or such other factors as the Director determines to be appropriate.

''(3) EXCLUDED SYSTEMS.—The Director of the National Institute of Standards and Technology may exclude from the requirements of paragraph (1) any computer hardware or software system for which the Director determines that the development of a checklist is inappropriate because of the infrequency of use of the system, the obsolescence of the system, or the inutility or impracticability of developing a checklist for the system.

''(4) AUTOMATION SPECIFICATIONS.—The Director of the National Institute of Standards and Technology shall develop automated security specifications (such as the Security Content Automation Protocol) with respect to checklist content and associated security related data.

''(5) DISSEMINATION OF CHECKLISTS.—The Director of the National Institute of Standards and Technology shall ensure that Federal agencies are informed of the availability of any product developed or identified under the National Checklist Program for any information system, including the Security Content Automation Protocol and other automated security specifications.

''(6) AGENCY USE REQUIREMENTS.—The development of a checklist under paragraph (1) for a

computer hardware or software system does not—

''(A) require any Federal agency to select the specific settings or options recommended by the checklist for the system;

''(B) establish conditions or prerequisites for Federal agency procurement or deployment of any such system;

''(C) imply an endorsement of any such system by the Director of the National Institute of Standards and Technology; or

''(D) preclude any Federal agency from procuring or deploying other computer hardware or software systems for which no such checklist has been developed or identified under paragraph (1).''.

SEC. 110. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY CYBERSECURITY RESEARCH AND DEVELOPMENT.

Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is amended by redesignating subsection (e) as subsection (f), and by inserting after subsection (d) the following:

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

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

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

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

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

TITLE II—ADVANCEMENT OF CYBERSECURITY TECHNICAL STANDARDS

SEC. 201. DEFINITIONS.

In this title:

(1) DIRECTOR.—The term ''Director'' means the Director of the National Institute of Standards and Technology.

(2) INSTITUTE.—The term ''Institute'' means the National Institute of Standards and Technology.

SEC. 202. INTERNATIONAL CYBERSECURITY TECHNICAL STANDARDS.

The Director, in coordination with appropriate Federal authorities, shall—

(1) ensure coordination of United States Government representation in the international development of technical standards related to cybersecurity; and

(2) not later than 1 year after the date of enactment of this Act, develop and transmit to the Congress a proactive plan to engage international standards bodies with respect to the development of technical standards related to cybersecurity.

SEC. 203. PROMOTING CYBERSECURITY AWARENESS AND EDUCATION.

(a) PROGRAM.—The Director, in collaboration with relevant Federal agencies, industry, educational institutions, and other organizations, shall develop and implement a cybersecurity awareness and education program to increase public awareness of cybersecurity risks, consequences, and best practices through—

(1) the widespread dissemination of cybersecurity technical standards and best practices identified by the Institute; and

(2) efforts to make cybersecurity technical standards and best practices usable by individuals, small to medium-sized businesses, State, local, and tribal governments, and educational institutions.

(b) MANUFACTURING EXTENSION PARTNERSHIP.—The Director shall, to the extent appropriate, implement subsection (a) through the Manufacturing Extension Partnership program under section 25 of the National Institute of Standards and Technology Act (15 U.S.C. 278k).

(c) REPORT TO CONGRESS.—Not later than 90 days after the date of enactment of this Act, the Director shall transmit to the Congress a report containing a strategy for implementation of this section.

SEC. 204. IDENTITY MANAGEMENT RESEARCH AND DEVELOPMENT.

The Director shall establish a program to support the development of technical standards, metrology, testbeds, and conformance criteria, taking into account appropriate user concerns, to—

(1) improve interoperability among identity management technologies;

(2) strengthen authentication methods of identity management systems;

(3) improve privacy protection in identity management systems, including health information technology systems, through authentication and security protocols; and

(4) improve the usability of identity management systems.

The CHAIR. No amendment to the committee amendment is in order except those printed in House Report 111–410. Each amendment may be offered only in the order printed in the report, by a Member designated in the report, shall be considered read, shall be debatable for the time specified in the report equally divided and controlled by the proponent and an opponent, shall not be subject to amendment, and shall not be subject to a demand for division of the question.

AMENDMENT NO. 1 OFFERED BY MR. HASTINGS OF FLORIDA

The CHAIR. It is now in order to consider amendment No. 1 printed in House Report 111–410.

Mr. HASTINGS of Florida. Madam Chair, I have an amendment at the desk.

The CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Amendment No. 1 offered by Mr. HASTINGS of Florida:

Page 21, line 4, strike ''and an'' and insert ''an''.

Page 21, line 8, insert '', and a description of how successful programs are engaging the talents of women and African-Americans, Hispanics, and Native Americans in the cybersecurity workforce'' after ''private sector''.

Page 23, line 11, insert '', and shall include representatives from minority-serving institutions'' after ''in cybersecurity''.

The CHAIR. Pursuant to House Resolution 1051, the gentleman from Florida (Mr. HASTINGS) and a Member in opposition each will control 5 minutes.

The Chair recognizes the gentleman from Florida.

Mr. HASTINGS of Florida. First, let me thank BART GORDON and this committee for the extraordinary work that they have done. And even though all of us are going to get an opportunity to say to the chairperson our thanks for his efforts here in Congress, I'd like to just personally thank him not only for the Cybersecurity Enhancement Act of 2009, but for substantial and substantive legislation throughout the course of his career.

I'm pleased to offer this amendment to address cybersecurity workforce concerns and advance the development of technical standards. If we're going to do that, we need to consider all of the different innovative opportunities out there. I was disappointed, though, to discover the significant gender and racial disparities in the cybersecurity industry.

We know cyberspace touches practically everything and everyone, yet I find it mind-boggling that we haven't made more of an effort to include everyone in protecting it. Women now constitute 50.7 percent of the U.S. population as of 2008, and the U.S. Census Bureau found that only 14 percent of women pursue professional careers in science or technology. Other underrepresented groups mentioned in this amendment include African Americans, Hispanics, and Native Americans. All of these groups have historically been underrepresented in scientific and engineering occupations. The U.S. Census Bureau recorded African Americans, Hispanics, and Native Americans as 28.2 percent of the U.S. population in 2008, yet these groups only represent a mere 10 percent of the science and technology industry.

In order to protect cyberspace, we need a strong vision and leadership. Both will require changes in policy, technology, education, and perhaps law. This bill will be recruiting the best and brightest, and we must ensure these opportunities are available to all Americans.

This amendment will address existing and potential racial and gender disparities in the industry. The first part of the amendment deals with the section on the cybersecurity workforce assessment. In this section, we require the President to transmit to Congress a report analyzing the cybersecurity workforce needs of the Federal Government. If we're going to take a good look at the sources and availability of cybersecurity talent in our country, then we must also take a more vigilant look at how we are including the talent of minorities.

According to a 1995 report by the National Research Council, ''limited access is the first hurdle faced by women seeking industrial jobs in science and engineering, and while progress has been made in recent years, common recruitment and hiring practices that make extensive use of traditional networks often overlook the available pool of women.'' Madam Chair, it is truly embarrassing that 15 years later, we find ourselves having made such little progress on this issue.

The second part of the amendment adds a requirement to include representatives from minority-serving institutions on the Cybersecurity University-Industry Task Force. In order to conduct a national dialogue on cybersecurity and develop more public awareness of the threat and risk, we need an integrated approach—one that includes a diverse industry that can

tackle our vulnerabilities while also meeting our economic needs and national security requirements.

Madam Chair, the United States needs a comprehensive framework to ensure a coordinated response and recovery by the government, the private sector, and our allies to a significant incident or threat. This amendment ensures that the process is accessible to our Nation's diverse talent.

In addition to thanking the committee, and especially Chairman GORDON, I'd like to thank our colleague, Congressman CIRO RODRIGUEZ of Texas for cosponsoring this amendment.

I urge my colleagues to support this effort.

Mr. MCCAUL. Madam Chair, I rise to claim time in opposition, although I do not intend to oppose this amendment.

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

There was no objection.

Mr. MCCAUL. Mr. HASTINGS and my colleague from Texas (Mr. RODRIGUEZ) are making improvements to this bill to ensure that the strategic plan takes into consideration the talents of women and minority populations in the cybersecurity workforce and that the University-Industry Task Force includes representatives from minority-serving institutions. I therefore urge support for this amendment.

I reserve the balance of my time.

□ 1345

Mr. HASTINGS of Florida. Madam Chair, I yield 30 seconds to the distinguished chairperson of the committee.

Mr. GORDON of Tennessee. Madam Chairman, first of all, let me thank my friend from Florida for his very kind words. But more importantly, I want to thank him for introducing this important legislation. We can have the best technology in the world, but if we don't have the workforce to go with it, then the bad guys win. This will go a long way to improving and expanding our workforce, and I thank the gentleman for this amendment.

Mr. RODRIGUEZ. Madam Chair, I rise in support of the Hastings-Rodriguez Amendment to H.R. 4061, the Cyber Security Enhancement Act.

Our amendment aims to address the lack of minority representation in the cyber security industry. In addition it provides for a minority serving institution to participate in the university-industry task force authorized by this legislation.

Our country is blessed to have many top-notch universities already training our future cyber security experts. For example, a minority serving institution in my district, the University of Texas—San Antonio, is producing both undergrads and graduate degrees in information assurance and computer science. UTSA has been designated a Center of Academic Excellence in Information Assurance Education and a Center of Academic Excellence in Information Assurance Research by the National Security Agency and Department of Homeland Security. Only 23 programs in the nation have achieved the research designation.

Universities like UTSA can play a major role in our national cyber policy and the training of our future cyber workforce. This underlying legislation will set us on our way to prepare our diverse workforce for our current and future needs.

I would like to thank my colleague Mr. HASTINGS for his partnership on this amendment. I urge my colleagues to support the Hastings/Rodriguez amendment and support H.R. 4061.

Mr. HASTINGS of Florida. Madam Chair, I yield back the balance of my time.

Mr. MCCAUL. I yield back the balance of my time.

The CHAIR. The question is on the amendment offered by the gentleman from Florida (Mr. HASTINGS).

The question was taken; and the Chair announced that the ayes appeared to have it.

Mr. HASTINGS of Florida. Madam Chairman, I demand a recorded vote.

The CHAIR. Pursuant to clause 6 of rule XVIII, further proceedings on the amendment offered by the gentleman from Florida will be postponed.

AMENDMENT NO. 2 OFFERED BY MR. GORDON OF TENNESSEE

The CHAIR. It is now in order to consider amendment No. 2 printed in House Report 111–410.

Mr. GORDON of Tennessee. Madam Chair, as the designee of the gentleman from Colorado, I rise to offer his amendment.

The CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Amendment No. 2 offered by Mr. GORDON of Tennessee:

Page 13, line 22, insert ''or, at the discretion of the Director, with appropriate private sector entities'' after ''technology workforce''.

The CHAIR. Pursuant to House Resolution 1051, the gentleman from Tennessee (Mr. GORDON) and a Member in opposition each will control 5 minutes.

The Chair recognizes the gentleman from Tennessee.

Mr. GORDON of Tennessee. Madam Chair, one of the best ways for cybersecurity professionals to improve their skills is through meaningful and diverse experiences. This amendment would allow scholarship recipients to seek out internship opportunities in the private sector and then bring those experiences to their service in the Federal Government.

I want to thank my friend Mr. POLIS for this good amendment, and I urge my colleagues to support it.

I yield back the balance of my time.

Mr. MCCAUL. Madam Chair, I rise to claim time in opposition, although I do not intend to oppose this amendment.

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

There was no objection.

Mr. MCCAUL. As part of the Scholarship for Service program at NSF, scholarship awardees are to receive internships at Federal agencies. This amendment simply gives the director the discretion of allowing them to intern in the private sector. So, therefore, I support this amendment.

I yield back the balance of my time.

The CHAIR. The question is on the amendment offered by the gentleman from Tennessee (Mr. GORDON).

The amendment was agreed to.

AMENDMENT NO. 3 OFFERED BY MR. FLAKE

The CHAIR. It is now in order to consider amendment No. 3 printed in House Report 111–410.

Mr. FLAKE. Madam Chair, I have an amendment at the desk, designated as No. 3 under the rule.

The CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Amendment No. 3 offered by Mr. FLAKE:

Page 12, after line 25, insert the following new subsection:

(h) PROHIBITION ON EARMARKS.—None of the funds appropriated under this section, and the amendments made by this section may be used for a Congressional earmark as defined in clause 9(d) of rule XXI of the Rules of the House of Representatives.

The CHAIR. Pursuant to House Resolution 1051, the gentleman from Arizona (Mr. FLAKE) and a Member in opposition each will control 5 minutes.

The Chair recognizes the gentleman from Arizona.

Mr. FLAKE. Madam Chair, this amendment, I hope, is noncontroversial in nature. Section 105 of the bill would authorize appropriations for several National Science Foundation grant programs dealing with cybersecurity. For example, the bill authorizes nearly $400 million through 2014 for computer and network security research grants. In addition, the bill would authorize such sums as necessary to make grants related to computer and network security research centers and capacity building, Scientific and Advanced Technology Act grants, and traineeships and research fellowships. This amendment would simply prohibit any earmarking of the funds made available for these programs under this act.

It appears that the grants are already intended to be awarded on a ''merit-reviewed competitive basis.'' But I think we still need this amendment because we've seen in the past, time and time and time and time again, that programs that were set up to be competitive accounts that are supposed to be competitive or merit reviewed are simply earmarked later. So if we have this language in it, it will make it less likely that these accounts are subject to earmarking. It's unfortunate that we have to take this step, I realize, but I think we should.

I agree with the President when he said last week that we need to ''continue down the path to earmark reform'' and that ''restoring the public trust demands more.'' This is doing more. I think that we ought to go much further than this, but this is a good start.

I wish to yield as much time as he may consume to the ranking minority member for his comments.

Mr. MCCAUL. Madam Chair, I rise in support of this amendment, and I also support the gentleman's position on earmarks. This amendment would prohibit the earmarking of the NSF and NIST cybersecurity activities authorized in this bill. It is well understood that awarding grants through merit-based competitive processes is the best way to fund science and technology, and cybersecurity is certainly no exception. This insulation from political influences is, in fact, an important reason why NSF and NIST have such a strong reputation overall both within and outside of the Federal Government.

Mr. FLAKE's amendment will help ensure that this model is being protected by incorporating it specifically into the statute. I urge my colleagues to support this amendment.

Mr. FLAKE. I thank the gentleman. Let me just say, I mentioned that we have had examples in the past. Let me just give one where programs that were supposed to be competitively awarded were, in fact, earmarked. Last year we established a grant program called the Emergency Operation Centers. It was established by Congress in FY 2008, in the Homeland Security bill. Last year in the spending bill, it showed that 60 percent of the funds in this grant program were earmarked. We simply can't allow that to happen here. This is a $400 million authorization for this grant program, and we can't have it earmarked.

I reserve the balance of my time.

Mr. GORDON of Tennessee. I rise to claim time in opposition to the amendment, even though I am not opposed to the amendment.

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

There was no objection.

Mr. GORDON of Tennessee. Madam Chairman, I want to thank my friend for introducing this amendment. It certainly is accepted by the majority; and I want to assure him, as Mr. MCCAUL can also, that this particular bill is clean as a whistle. There are no earmarks, NSF, NIST, or anywhere else. Again, I thank him for making sure that we get that clarified.

I yield the balance of my time to the gentleman from Colorado (Mr. POLIS).

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

Mr. POLIS. Thank you, Chairman GORDON. Madam Chair, I rise today in support of the Polis amendment to H.R. 4061, the Cybersecurity Enhancement Act of 2009. We enjoyed working very closely with Chairman GORDON, his staff, Representative LIPINSKI; and I appreciate their leadership on this critical and bipartisan bill that will train the experts who we need to tackle tomorrow's challenges and enable the United States and the world to stay competitive in cybersecurity.

In a world of blogs and widgets, smartphones and email, we are truly a global community, growing ever-closer and ever-more interconnected. The average citizen cannot help but feel part of an extended electronic family. Technological progress has enhanced our personal and work lives regardless of our job or position. As someone who has founded and run several small technology-related businesses, I can speak to the advantages of working in the technology age and how it's improved my ability now on the political side to represent the people of Colorado's Second Congressional District.

My amendment expands the proposed internship opportunities available to participants in the Federal Cyber Scholarship for Service program to include placements in the private sector. I believe it will serve tomorrow's cybersecurity professionals and our national security interests to open up this program to a diversity of experience from the public and private sector. For the future recipients of these scholarships, it will provide the occasion to serve not only in the Federal technology workforce but also at the abundance of small, medium and large businesses that help make up our Nation's economy.

My district is a great example of where institutions of higher education, small business and the Federal Government cooperate to benefit one another and the rest of the Nation. We have a thriving community of startups, lower than average unemployment and a history of growing successful small businesses. With the collaboration of budding cybersecurity professionals from the University of Colorado in Boulder, these companies can benefit from their education and, in turn, impart the practical knowledge that will build each student's portfolio of experience. Having gained and grown from these experiences, I am positive that their education in the private sector will help promote unique solutions to daunting tasks during their time in the Federal Government. What originally seemed like a strategy only applicable to small high-tech companies in Boulder can now serve as a useful tool when confronted with the task of fending off cyberattacks from nation-states or rogue individuals.

The state of cybersecurity is fast becoming one of the greatest challenges of the 21st century. It's apparent that despite increased spending on research and development, our technological infrastructure is still vulnerable. China's recent intrusion into Google's operations should serve as a call for preparedness to both the private sector and the Federal Government.

This past May, President Obama's cyberspace policy review highlighted the importance of developing partnerships between the Federal Government and the private sector. The limits of cybergrowth are constantly expanding and so too must our plans to address the plethora of issues that crop up. As Secretary Clinton put it recently: ''The Internet, though a blessing, can be a threat to those who would fall prey to cyberterrorism.'' It is our job, as inventors and stewards of the Internet, to ensure unhindered, free and secure access to enrich the lives of everyone.

By boosting our training capabilities, we are helping to ensure a safe and free Internet experience. This amendment helps to guarantee that we are addressing the long-term challenges inherent in cybersecurity. It will create ties to the private sector and cultivate a workforce for the future. Madam Chairman, this amendment and this bill are critical to protecting our Nation's sensitive information and ensuring our cybersecurity. I appreciate the Committee of the Whole for accepting this amendment and Mr. GORDON for offering it.

Mr. FLAKE. Just to conclude, I appreciate the majority's willingness to accept the amendment. Again, I appreciate the fact that there are no earmarks in this authorization. What we're seeking to do here is that when money is appropriated for these programs that are authorized here, that none of that money can be earmarked like we've seen in many, many, many bills before.

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

Mr. GORDON of Tennessee. I yield back the balance of my time.

The CHAIR. The question is on the amendment offered by the gentleman from Arizona (Mr. FLAKE).

The question was taken; and the Chair announced that the ayes appeared to have it.

Mr. GORDON of Tennessee. Madam Chairman, I demand a recorded vote.

The CHAIR. Pursuant to clause 6 of rule XVIII, further proceedings on the amendment offered by the gentleman from Arizona will be postponed.

AMENDMENT NO. 4 OFFERED BY MR. MATHESON

The CHAIR. It is now in order to consider amendment No. 4 printed in House Report 111–410.

Mr. MATHESON. I have an amendment at the desk.

The CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Amendment No. 4 offered by Mr. MATHESON:

Page 9, line 23, strike ''is amended'' and insert ''is amended—

(1)''.

Page 9, line 25, strike the period and insert ''; and''.

Page 9, after line 25, insert the following new paragraph:

(2) by amending subparagraph (I) to read as follows:

''(I) enhancement of the ability of law enforcement to detect, investigate, and prosecute cyber-crimes, including crimes that involve piracy of intellectual property, crimes against children, and organized crime.''.

The CHAIR. Pursuant to House Resolution 1051, the gentleman from Utah (Mr. MATHESON) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentleman from Utah.

Mr. MATHESON. Madam Chair, I will be very brief. You know, right now this legislation to enhance cybersecurity authorizes the National Science Foundation to assist in doing research that will help law enforcement look for issues related to intellectual property. I thought it would be helpful if we also included and amended this bill to enhance the ability of law enforcement to prosecute cybercrimes that involve crimes against children and organized crime.

So simply stated, that is the substance of this amendment. I think any of us who are parents of children right now have concerns about when kids are using the Internet and the amount of inappropriate material that's on it right now and the number of folks who are targeting children on the Internet. So I thought that would be a helpful amendment to this bill. I encourage my colleagues to support this amendment.

I reserve the balance of my time.

Mr. MCCAUL. Madam Chair, I rise to claim time in opposition, although I am not opposed to this amendment.

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

There was no objection.

Mr. MCCAUL. Madam Chair, NSF computer and network security research grants are intended to enhance computer security through basic hardware and software research in numerous areas, including the ability for law enforcement to detect, investigate, and prosecute cybercrimes.

This amendment merely highlights crimes against children and organized crime, such as cybercrimes, where these investments should be made. So I fully support this good amendment.

I yield back the balance of my time.

Mr. MATHESON. I yield back the balance of my time as well, Madam Chair.

The CHAIR. The question is on the amendment offered by the gentleman from Utah (Mr. MATHESON).

The amendment was agreed to.

AMENDMENT NO. 5 OFFERED BY MR. ROSKAM

The CHAIR. It is now in order to consider amendment No. 5 printed in House Report 111–410.

Mr. ROSKAM. Madam Chair, I have an amendment at the desk.

The CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Amendment No. 5 offered by Mr. ROSKAM:

Page 8, line 20, insert ''and community colleges'' after ''minority serving institutions''.

Page 14, line 10, insert ''and community colleges'' after ''minority serving institutions''.

Page 21, line 6, insert '', including community colleges,'' after ''institutions of higher education''.

Page 23, line 10, insert '', including community colleges,'' after ''institutions of higher education''.

The CHAIR. Pursuant to House Resolution 1051, the gentleman from Illinois (Mr. ROSKAM) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentleman from Illinois.

Mr. ROSKAM. I yield myself such time as I may consume.

Madam Chair, I thank the majority for making this amendment in order and a special thank you to the gentleman from Illinois (Mr. LIPINSKI) who was instrumental in putting this together.

The amendment is actually very straightforward and very, very simple. It just inserts the word or phrase ''community college'' at four different points in the bill.

□ 1400

What this amendment is trying to do is to expand the pool of people that we're reaching out to to bring into this idea of taking on this great challenge of cybersecurity. In a nutshell, I'd like to read just a quick paragraph from a community college in my district, the College of DuPage, located in Glen Ellyn, Illinois. It says of this amendment that it will capitalize on the abilities of the exceptional faculty, talented students, and the state-of-the-art facilities at the College of DuPage and institutions like it to produce careers and put in place systems to protect our country. And similarly, the amendment is supported by the American Association of Community Colleges.

But I think, putting this into a larger context, it's important, because if you look at where we're going as a Nation, and notwithstanding all the turmoil that we've seen regarding our economy and where we're attempting to go, and we're struggling with great unemployment rates and so forth, without question, it's the technology sector of our economy that's going to lead the way. And without question, we're going to need an underlying system that is secure. And so I think casting a wider net, including folks in the community college system who have proven themselves time and time again, to ultimately invite them into this solution, I think, is the way to go. It's a fairly straightforward amendment and it says that technology is important for our Nation and, ultimately, technology and cybersecurity are important for our Nation.

I yield to the gentleman from Texas (Mr. MCCAUL) for such time as he may consume.

Mr. MCCAUL. Madam Chairman, I'm pleased to strongly support this amendment. Our Nation's community colleges have played a crucial role in our technology and educational workforce. This amendment makes sure they are able to make recommendations and give advice to the Federal Government on the strategic plan. It emphasizes their eligibility as a potential institutional partner under the Scholarship for Service Program and really puts them at the table of the University-Industry Task Force.

So, with that, I strongly urge support.

Mr. ROSKAM. I thank the gentleman for his kind words.

I yield back the balance of my time.

The CHAIR. The question is on the amendment offered by the gentleman from Illinois (Mr. ROSKAM).

The amendment was agreed to.

AMENDMENT NO. 6 OFFERED BY MS. EDWARDS OF MARYLAND

The CHAIR. It is now in order to consider amendment No. 6 printed in House Report 111–410.

Ms. EDWARDS of Maryland. Madam Chairman, I have an amendment at the desk.

The CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Amendment No. 6 offered by Ms. EDWARDS of Maryland:

At the end of the bill, insert the following new section:

SEC. 205. PRACTICES AND STANDARDS.

The National Institute of Standards and Technology shall work with other Federal, State, and private sector partners, as appropriate, to develop a framework that States may follow in order to achieve effective cybersecurity practices in a timely and cost effective manner.

The CHAIR. Pursuant to House Resolution 1051, the gentlewoman from Maryland (Ms. EDWARDS) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentlewoman from Maryland.

Ms. EDWARDS of Maryland. Madam Chairman, I want to take this moment to thank Chairman GORDON and Ranking Member HALL and Representative LIPINSKI for their hard work on this really important bill and for consideration of this amendment. I probably, like lots of Americans, have faced the circumstance, even in this last month and a half, private information compromised first at a bank, then at a Federal agency, and then at a retail establishment, all within the span of a month and a half.

Threats such as identity theft, denial of service attacks, worms, viruses, the loss of sensitive information, and other malicious activity are a part of the ever-evolving cybersecurity threat to our country. It's important that we act swiftly to prepare our Nation for these threats and to anticipate the threats that we'll face in the years to come. It's not an easy task. We operate on a system of databases throughout this country that interact at the Federal, State, and local level and in the commercial sector.

This bipartisan bill really accomplishes all of these goals. And further, the amendment that I'm offering really encourages the National Institute of Standards and Technology to work with other Federal Government entities, State governments and the private sector partners to develop a framework that States may follow as they strengthen their cybersecurity standards.

One of the weaknesses identified as our committee marked up this legislation is the lack of collaboration between various entities concerned with

cybersecurity. The underlying bill takes major steps to address this, but I believe that my amendment strengthens these measures and will lead to States that are many times on the front lines to make major progress toward keeping their networks and information safe; and, of course, that does trickle down to the local level and out into the commercial sector.

In my home State of Maryland, we just made a major commitment to cybersecurity, as many States have across this country, with varying standards of operation and security around the country. This amendment will ensure that States can use their resources much more efficiently. Security requirements and priorities are unique to each State and often times unique among government entities in the same State. My amendment recognizes this and allows States and the standards to adapt with the changing threats and needs.

Madam Chairman, I urge my colleagues to support this amendment because we must encourage collaboration and innovation as we aim to address the multiple threats to our cybersecurity.

I reserve the balance of my time.

Mr. MCCAUL. Mr. Chairman, I rise to claim time in opposition to this amendment, although I am not opposed to it.

The Acting CHAIR (Mr. MORAN of Virginia). Without objection, the gentleman from Texas is recognized for 5 minutes.

There was no objection.

Mr. MCCAUL. This amendment directs NIST to work with Federal, State, and private-sector partners to develop a framework that States may use to improve their cybersecurity posture. Developing such a framework for use in assisting States is certainly consistent with NIST's expertise and capabilities, and there is clearly a need for this expertise at the State level.

I should note, in working with the States, that we should, of course, expect that the NIST role remains limited to the development of guidance that the States may use, if they choose, avoiding any activities that are mandatory or binding in nature.

I'd like to yield to the gentlelady from Maryland (Ms. EDWARDS) to say if that's a correct statement. That is my understanding of this amendment.

Ms. EDWARDS of Maryland. That's correct.

Mr. MCCAUL. Reclaiming my time then, I'm comfortable with the language in this amendment as written and very much support its passage.

I yield back the balance of my time.

Ms. EDWARDS of Maryland. Mr. Chairman, I'd like to yield 30 seconds to the chairman, the gentleman from Tennessee (Mr. GORDON).

Mr. GORDON of Tennessee. Mr. Chairman, I thank my friend from Maryland, and I want to thank her more importantly for introducing this commonsense constructive amendment that's going to provide additional tools for the States as they fight this issue, very well pointed out, this very difficult, day-to-day battle with cybersecurity.

Ms. EDWARDS of Maryland. Mr. Chairman, I would like to just conclude by saying that it's really important that we get this right at every level because of increasing threats to our cybersecurity, both internationally and here domestically. And I urge, again, my colleagues for careful consideration and approval of this amendment.

I yield back the balance of my time.

The Acting CHAIR. The question is on the amendment offered by the gentlewoman from Maryland (Ms. EDWARDS).

The amendment was agreed to.

AMENDMENT NO. 7 OFFERED BY MR. PAULSEN

The Acting CHAIR. It is now in order to consider amendment No. 7 printed in House Report 111–410.

Mr. PAULSEN. 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:

Amendment No. 7 offered by Mr. PAULSEN:

Page 7, line 15, strike ''and''.

Page 7, line 20, strike the period and insert ''; and''.

Page 7, after line 20, insert the following new paragraph:

(7) outline how the United States can work strategically with our international partners on cybersecurity research and development issues where appropriate.

The Acting CHAIR. Pursuant to House Resolution 1051, the gentleman from Minnesota (Mr. PAULSEN) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentleman from Minnesota.

Mr. PAULSEN. Mr. Chairman, I yield myself as much time as I may consume.

Mr. Chairman, I rise today to offer an amendment that would require that the cybersecurity strategic research and development plan to also include how we can work with international partners to make our technology infrastructure even safer.

Throughout most of our Nation's history, our security concerns have evolved around our national security of military security, intelligence, and protection of our borders. Now, over the past few decades, our technological advances and our ever-increasing reliance on that technology are increasingly important and have drastically expanded. This, naturally, makes our technology a likely target for attack by those that would like to harm the United States.

Furthermore, as Minnesota's Chief Information Officer, Gopal Khanna, says, ''Cybersecurity is not just a Federal issue; it is also a national policy issue with huge global ramifications.'' And he is absolutely correct, Mr. Chairman. We must view the issue of cybersecurity from both a domestic and a foreign perspective. His article, ''Mutually Assured Survival in Cyber Space,'' which I do intend to offer into the RECORD, outlines the critical importance of our Nation's cybersecurity infrastructure.

As Mr. Khanna states, a cybersecurity attack on our most vulnerable assets—that's the data and information that power our productivity and support the United States and global economies—will be utterly devastating. An attack would not only affect us here at home, but it would have a very adverse impact on our trading partners and the flow of commerce every day.

Today's technology-driven economy makes cybersecurity an essential national security issue, one with ramifications that stretch across our Nation and far beyond our borders. We must remember this as we look at ways to strengthen cybersecurity. We need to think about our alliances abroad in the general context of new geopolitical realities of the digital cyberworld in which we live and operate today, and this amendment recognizes those realities.

[From Governing, Sept. 8, 2009]

MUTUALLY ASSURED SURVIVAL IN CYBER SPACE

(By Gopal Khanna)

We must pool resources to focus on an all-encompassing national approach to defending our information infrastructure from attacks.

For the better part of the 20th century, America's greatest threat came from the expansionist strategies of Communism, with its values and aspirations so contradictory to our own free and open democratic society. At the heart of the conflict was the proliferation of nuclear arsenals and the horrific potential to kill millions with one strike. Baby boomers who were schoolchildren at the time remember the drills when they were instructed to hide under their desks in the event of an attack.

While nuclear proliferation is still a threat, America is beginning to recognize a sleeper threat of a different kind: the devastation that can result from the mass disruption of business communications and the workings of government through cyber attacks. As we reflect on the results of President Obama's 60-day Cyberspace Policy Review, policy makers and private-sector leaders need to come together to apply great effort and creativity in crafting safeguards against these vulnerabilities.

The series of apparently orchestrated attacks on U.S. Web sites in July—directed at such critical entities as the Treasury Department, Secret Service, Federal Trade Commission and New York Stock Exchange—is precisely why the U.S. should become a leader in thwarting cyber attacks on our national and international information infrastructure. In his May 29 remarks on securing the nation's information infrastructure, President Obama stated that ''the status quo is no longer acceptable'' and called our attention to the critical work ahead. To reiterate that point, last month Homeland Security Secretary Janet Napolitano emphasized how important the role of state and local governments will be in meeting today's cyber security threats and that ''it is important to recognize that there is no international structure'' where cyber crime is concerned.

The Cyberspace Policy Review has validated our understanding that it is not only corporate America that is now under siege, but the federal, state and local governments, private institutions and non-governmental organizations as well. Capable of wreaking a different sort of havoc, and easier to execute, today's menace comes from cyber security attacks on our most valuable assets—the data and information that power our productivity and support the economy of the United States and the world.

That is why we must pool resources to focus on an all-encompassing national approach to defending our assets within the context of the new geopolitical realities of the digital world we live in. We need to apply all of our tools and our finest minds to harness our capabilities and competencies in the interest of protecting an infrastructure that supports our way of life. Just as ducking under desks would have done little to protect schoolchildren in the 1950s from a nuclear attack, simply hiding behind new software or the latest firewall will not protect us from tomorrow's range of cyber threats. We must do more.

To this end, the United States should take the lead in an international endeavor to address these threats; not only the risks to our own country but also the risks to our allies in free economies and open governments around the world. Every attack, regardless of its target, poses global dangers, due to the interconnections of digital infrastructure and networks as well as the interdependencies of national and regional economies, and imperils commerce and communications among all nations.

In the past, the doctrine of Mutually Assured Destruction acted as a deterrent to prevent a nuclear first-strike by either side. Both the United States and the Soviet Union knew that a strike would mean mutual annihilation. As a result, although the doctrine has not contained the spread of nuclear technology to rogue states, a nuclear weapon has not been detonated in military conflict since World War II.

We need to develop an analogous approach against these new dangers—one that fends off the cyber anarchy envisioned by some nation-states and fringe borderless entities.

The G–20 Summit in Pittsburgh this month is an ideal forum to establish America's leadership in cyber security. It's important that the international community come together to answer some basic, foundational questions about cyber attacks as a tactic of warfare: Should attacks of a cyber-nature be condemned in the same manner as chemical and biological weapons? How should a country respond to a cyber attack from another nation-state? How should the international community respond to such an attack?

The potential for mass disruption to all aspects of social, economic and political workings of nations requires that the G–20 country CIOs who are responsible for policies, practices and management of the digital infrastructure in their respective jurisdictions be a part of this discussion.

By working together, perhaps it will be understood that a cyber attack against one country is an attack against all countries, justifying a response—maybe even an international response. Time will tell if the international community will embrace as bold a deterrent as ''Mutually Assured Survival in Cyber Space.'' Still, now is the time to develop a doctrine of accountability and consequences that will serve as a deterrent to nation-states and rogue entities and prevent levels of cyber warfare that could jeopardize international trade, our government services, our security, our corporate and business interests, and most important, our open, democratic way of life.

I yield such time as he may consume to my colleague from Texas (Mr. MCCAUL).

Mr. MCCAUL. Mr. Chairman, I rise in strong support of this amendment. The gentleman is absolutely correct. The Internet knows no boundaries. This is not just an issue for the United States; it's a global issue that we need to address. This amendment simply states that the interagency cybersecurity R&D plan required by the legislation outlines how the United States can work strategically with international partners on cybersecurity R&D.

Cybersecurity issues are certainly global in nature. Many of our closest allies face the same threats and vulnerabilities that we do. Thus, it makes sense that we should work to cooperate more closely with our international partners, and that is what this amendment will do. Therefore, I strongly urge support.

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

Mr. GORDON of Tennessee. Mr. Chairman, I claim the time in opposition to the amendment, even though I'm not opposed to the amendment.

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

There was no objection.

Mr. GORDON of Tennessee. Mr. Chairman, I concur with Mr. MCCAUL in saying that cyberthreats know no boundaries. This is, again, a good commonsense amendment, and I thank the gentleman from Minnesota (Mr. PAULSEN) for introducing it, and we support the amendment.

I yield back the balance of my time.

Mr. PAULSEN. Mr. Chairman, just in closing, I know that by working together on the commonsense approach—I thank the gentleman—I look forward to support of this amendment.

I yield back the balance of my time.

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

The amendment was agreed to.

AMENDMENT NO. 8 OFFERED BY MRS. DAHLKEMPER

The Acting CHAIR. It is now in order to consider amendment No. 8 printed in House Report 111–410.

Mrs. DAHLKEMPER. 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:

Amendment No. 8 offered by Mrs. DAHLKEMPER:

Page 12, after line 25, insert the following new subsection:

(h) COMPUTER AND NETWORK SECURITY CAPACITY BUILDING GRANTS—MANUFACTURING EXTENSION PARTNERSHIP.—Section 5(a)(3) of the Cyber Security Research and Development Act (15 U.S.C. 7404(a)(3)) is amended—

(1) by striking ''and'' at the end of subparagraph (I);

(2) by redesignating subparagraph (J) as subparagraph (K); and

(3) by inserting after subparagraph (I) the following new subparagraph:

''(J) establishing or enhancing collaboration in computer and network security between community colleges, universities, and Manufacturing Extension Partnership Centers; and''.

The Acting CHAIR. Pursuant to House Resolution 1051, the gentlewoman from Pennsylvania (Mrs. DAHLKEMPER) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentlewoman from Pennsylvania.

Mrs. DAHLKEMPER. Mr. Chairman, my amendment to H.R. 4061 expands computer and network security capacity, building grants to allow for collaboration between community colleges, universities, and Manufacturing Extension Partnership centers.

As we all know, cybersecurity is an issue that affects both our national security and our economic prosperity, and it poses a particular problem for our small businesses. Small and medium-sized businesses often cannot shoulder the costs of developing and maintaining the mechanisms needed to protect themselves from cybersecurity threats. Individually, the security of these firms may seem like a minor affair compared to larger economic and government entities; however, the 27 million small and medium-sized businesses across the country account for 95 percent of our Nation's business.

Collaboration will benefit all participants, from applied research and curriculum planning on the academic side to workforce training and better, more cost-efficient security measures for Manufacturing Extension Partnership centers and their industry partners.

I want to thank Representative GORDON, Ranking Member HALL, and Representative LIPINSKI for their leadership on this bill.

I urge my colleagues on both sides of the aisle to support the Cybersecurity Enhancement Act of 2009 and my amendment that will help small businesses, starting with our manufacturers, better confront the serious challenges of cyberspace security.

I reserve the remainder of my time.

Mr. MCCAUL. Mr. Chairman, I rise to claim time in opposition to this amendment, although I'm not opposed to it.

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

There was no objection.

Mr. MCCAUL. This amendment simply provides an establishing or enhancing cybersecurity collaboration between community colleges, universities, and NIST Manufacturing Extension Partnership centers, and is among the most eligible activities that may be supported by NSF cybersecurity research grants.

□ 1415

This collaboration between researchers and those that provide technical support regarding cybersecurity best practices is benefiting and should be encouraged. And therefore, I support

the gentlelady from Pennsylvania's amendment.

I yield back the balance of my time.

Mrs. DAHLKEMPER. I yield as much time as he may consume to the gentleman from Tennessee (Mr. GORDON).

Mr. GORDON of Tennessee. I thank my friend from Pennsylvania.

This is a very important amendment to our committee's work. The community colleges have so much potential to offer us, and I think by bringing this to the table we're going to bring a whole other sector to getting involved. And once again, this goes back to workforce issues. We can have the best technology in the world, but if we don't have the workforce to go with it, then we're not going to be successful.

So I thank the gentlelady for this excellent amendment.

Mrs. DAHLKEMPER. I yield back the remainder of my time.

The Acting CHAIR. The question is on the amendment offered by the gentlewoman from Pennsylvania (Mrs. DAHLKEMPER).

The question was taken; and the Acting Chair announced that the ayes appeared to have it.

Mrs. DAHLKEMPER. Mr. Chair, I demand a recorded vote.

The Acting CHAIR. Pursuant to clause 6 of rule XVIII, further proceedings on the amendment offered by the gentlewoman from Pennsylvania will be postponed.

AMENDMENT NO. 9 OFFERED BY MR. GARAMENDI

The Acting CHAIR. It is now in order to consider amendment No. 9 printed in House Report 111–410.

Mr. GARAMENDI. I rise for the purposes of offering an amendment.

The Acting CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Amendment No. 9 offered by Mr. GARAMENDI:

Page 28, line 21, and page 29, line 1, redesignate subsections (b) and (c) as subsections (c) and (d), respectively.

Page 28, after line 20, insert the following new subsection:

(b) WORKSHOPS.—In carrying out activities under subsection (a)(1), the Institute is authorized to host regional workshops to provide an overview of cybersecurity risks and best practices to businesses, State, local, and tribal governments, and educational institutions.

The Acting CHAIR. Pursuant to House Resolution 1051, the gentleman from California (Mr. GARAMENDI) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentleman from California.

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

Long ago, I learned as a Boy Scout you need to be prepared, but to be prepared, you need knowledge and information. This amendment is all about knowledge and information for the public.

About 70 percent of Californians are linked to the Internet, but that Internet brings great problems. A new infected Web page is discovered every 5 seconds; a new spam-related Web page is discovered every 20 seconds. And additionally, there are some 2,500 e-mail messages that contain infected information. So we best be prepared.

In order to do that, we need knowledge, and that is what this amendment is all about. It provides the opportunity for the Institute to carry out the Cybersecurity Awareness and Education Program by conducting workshops around the Nation. With those workshops available, the information can be disseminated and made available to individuals.

That is the thrust of the amendment, and I seek an ''aye'' vote.

I reserve the balance of my time.

Mr. MCCAUL. I rise to claim time in opposition to this amendment although I am not opposed to it.

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

There was no objection.

Mr. MCCAUL. This amendment specifies that as part of its outreach and education efforts NIST may host regional workshops on cybersecurity risks and best practices for businesses, State, and local governments and educational institutions.

I think that's a good thing, and while I do not oppose this amendment, I'd like to note that NIST has a very modest budget for cybersecurity activities, of which outreach and education is just a small fraction.

Accordingly, in carrying out the section of this bill is my expectation that this should work to leverage this funding to benefit the largest number of entities and individuals as it can. I recognize workshops can also serve as a useful outreach tool and should be an option.

So with that point in mind, I do not object to this amendment.

I yield back the balance of my time.

Mr. GARAMENDI. The gentleman points out some very good points that there are issues about the budget. I am sure that the Institute will find the very best way to carry out this particular task.

I yield such time as he may consume to the chairman of the committee.

Mr. GORDON of Tennessee. First, let me thank my friend from California for an excellent amendment. It's an improvement to an already-good bill.

Mr. Chairman, I rise now to offer my condolences to the family of Judy Ruckel. Judy was the printer for the Committee on Science and Technology, and she unexpectedly passed away earlier this week. Because she worked from home, I did not know Judy as well as I do other members of the staff. She was a quiet, often unseen stalwart of the committee. Most staff members never questioned how the documents that are the record of our work get produced, and it's a testament to Judy that they never had to. Judy just took care of it.

When I first became chairman, I had no idea what a committee printer did. I kept asking who the printer was, what did she do, where was her office. Universally I was told that Judy was the nicest, most caring person that you could ever have on your staff and that she was good at whatever she did and that I needed to have no concerns on that front. Everyone was right.

Judy's quiet presence and good work will be missed by all on our committee.

Mr. GARAMENDI. I yield back the balance of my time.

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

The amendment was agreed to.

AMENDMENT NO. 10 OFFERED BY MRS. MCCARTHY OF NEW YORK

The Acting CHAIR. It is now in order to consider amendment No. 10 printed in House Report 111–410.

Mrs. MCCARTHY of New York. I have an amendment at the desk.

The Acting CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Amendment No. 10 offered by Mrs. MCCARTHY of New York:

Page 28, line 20, insert '', especially with respect to novice computer users, elderly populations, low-income populations, and populations in areas of planned broadband expansion or deployment'' after ''educational institutions''.

The Acting CHAIR. Pursuant to House Resolution 1051, the gentlewoman from New York (Mrs. MCCARTHY) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentlewoman from New York.

Mrs. MCCARTHY of New York. I'd like to thank Chairman GORDON and Ranking Member HALL for bringing forward this important bill.

The images of growth and the Internet over the years has brought, and will continue to bring, new and exciting opportunities. While these opportunities, however, have new challenges for all of us, H.R. 4061, the Cyber-security Enhancement Act of 2009 is an important bill that will foster safer and more productive Internet use nationally.

I am so proud that the President, his administration, as well as my colleagues in Congress, have all made Internet innovation and security a priority. I am even more proud of the educational provisions in H.R. 4061 that, in my opinion, are vital to the successful growth and sustainability of the Internet and its many real-world applications.

Computer literacy may be something that some of us take for granted, but there are significant portions of our Nation that are unfamiliar with the full spectrum of dangers careless computer use can have.

Our daily lives have become increasingly reliant on the Internet, and over the years, Congress has made substantial investments in its growth. It is

only natural that Congress compliment this technological investment with targeted educational initiatives as well.

I am proud to offer, along with my esteemed colleague, Mr. KRATOVIL of Maryland, an amendment that will ensure that proper cybersecurity education efforts focus on those that need them most, namely new computer users, elderly and low-income populations, as well as those residing in areas of planned Internet expansion and deployment.

My amendment will do much to ensure that vulnerable populations receive due attention as part of a public awareness campaign for cybersecurity. According to the Pew Research Center, only a third of the elderly are considered to be Internet users. Moreover, the Pew Research Center finds that household income plays a significant factor in cyber literacy.

Too often we hear stories of those taken advantage of or ignorant to the dangers of the Internet. We have the opportunity to educate and prevent careless Web surfing.

Today, with my amendment, we, as a Nation, have an opportunity to ensure that those new and less experienced computer users are given the opportunity to be proactive members of the Internet community.

I reserve the balance of my time.

Mr. MCCAUL. I rise to claim time in opposition to this amendment, but do not intend to oppose it.

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

There was no objection.

Mr. MCCAUL. Mr. Chairman, this amendment simply States that the NIST Cybersecurity Awareness and Education Program established in the bill helps makes the technical standards and best practices more usable for everyone, especially those new to computers: The elderly, those with low incomes, and those that may not have broadband quite yet, such as rural areas. Therefore, I do not oppose this amendment.

I would like to join Chairman GORDON at this point in time to offer my sincere condolences as well to the family of Judy Ruckel.

Judy served as a printer for the Science and Technology Committee since 2001 under both Republican and Democratic leadership. Day in and day out, Judy carried out her job with style and grace and never did she allow her struggle with diabetes to diminish her presence nor her performance.

Judy worked from home, but during her visits to our offices each week, she took time to look in on staff, inquiring about our families and challenges, always leaving a smile on the faces of those she came in contact with.

The job of managing countless hearing transcripts and markups and transforming them into permanent records is absolutely critical to the life of our committee, and Judy did it to perfection. She is irreplaceable. Judy's suffering has ended, and we will miss her very deeply, and God be with her.

I yield back the balance of my time.

Mrs. MCCARTHY of New York. I'd like to yield as much time as he may consume to the gentleman from Illinois (Mr. LIPINSKI).

Mr. LIPINSKI. Every year, hundreds of thousands of people fall victim to Internet fraud so it's really clear we need to improve our cybersecurity awareness and education.

There are some who are especially vulnerable to falling victims to this fraud. So I think that this amendment by Mrs. MCCARTHY and Mr. KRATOVIL is a very good amendment.

I know that certainly I have seen and have had experience with people, especially those who are elderly, falling victim to crimes. I've had them come to my office and have problems about that and trying to clear that up.

So I think this is an especially good amendment, and I urge my colleagues to support it.

Mrs. MCCARTHY of New York. I urge all of my colleagues to support the amendment. I yield back the balance of my time.

The Acting CHAIR. The question is on the amendment offered by the gentlewoman from New York (Mrs. MCCARTHY).

The amendment was agreed to.

AMENDMENT NO. 11 OFFERED BY MS. LORETTA SANCHEZ OF CALIFORNIA

The Acting CHAIR. It is now in order to consider amendment No. 11 printed in House Report 111–410.

Ms. LORETTA SANCHEZ of California. Mr. Chairman, as the designee of Mr. SMITH from Washington, I rise to offer the amendment.

The Acting CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Amendment No. 11 offered by Ms. LORETTA SANCHEZ of California:

Page 21, line 21, insert ''job security clearance and suitability requirements,'' after ''job classification,''.

The Acting CHAIR. Pursuant to House Resolution 1051, the gentlewoman from California (Ms. LORETTA SANCHEZ) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentlewoman from California.

Ms. LORETTA SANCHEZ of California. I yield myself as much time as I may consume.

I rise in support of this amendment, which I am pleased to offer today on behalf of my colleague, Mr. SMITH of Washington, who is unable to be with us today due to a health issue.

I thank the gentleman for offering this amendment, which will strengthen our cybersecurity workforce, in turn protecting the security of our Nation.

Our country faces numerous cyberattacks each day, and as a result, we must ensure that our cyberworkforce not only possesses the knowledge and the skills necessary to defend our networks but also the ability to collaborate with the numerous departments and agencies within the Federal Government who lead the effort to combat these threats.

Information technology professionals at our civilian agencies who may not deal with classified information on a daily basis should be able to provide their expertise and have the ability to work with and discuss cyber-related issues with the Department of Defense and our intelligence community.

To that end, this amendment would modify Section 107 of the bill, which calls for the President to submit a report to Congress addressing the cybersecurity workforce needs of the Federal Government.

□ 1430

The amendment would require the report to also examine the current security clearance and job suitability requirements that may serve as a deterrent to hiring an adequately trained cyber-workforce.

Again, I want to wish Congressman SMITH a speedy recovery and encourage my colleagues to support this amendment.

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

Mr. MCCAUL. Mr. Chairman, I rise to claim time in opposition, although I'm not opposed to this amendment.

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

There was no objection.

Mr. MCCAUL. This amendment would include some additional factors to be considered in the assessment of the cybersecurity workforce and barriers to entry into that workforce. Job security clearance and suitability requirements are important factors to consider in this assessment. I thank the gentlelady for a constructive amendment.

I yield back the balance of my time.

Ms. LORETTA SANCHEZ of California. Mr. Chairman, I have no other speakers, and I would just ask to move this and for my colleagues to vote on it. And I yield back the balance of my time.

The Acting CHAIR. The question is on the amendment offered by the gentlewoman from California (Ms. LORETTA SANCHEZ).

The amendment was agreed to.

AMENDMENT NO. 12 OFFERED BY MR. LANGEVIN

The Acting CHAIR. It is now in order to consider amendment No. 12 printed in House Report 111–410.

Mr. LANGEVIN. I have an amendment at the desk.

The Acting CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Amendment No. 12 offered by Mr. LANGEVIN:

Page 21, line 25, insert '', including recommendations on the temporary assignment of private sector cybersecurity professionals to Federal agencies'' after ''cybersecurity workforce''.

The Acting CHAIR. Pursuant to House Resolution 1051, the gentleman

from Rhode Island (Mr. LANGEVIN) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentleman from Rhode Island.

Mr. LANGEVIN. Mr. Chairman, I rise today to offer an amendment to H.R. 4061 that would expand private sector involvement in our cybersecurity efforts. By now we should all recognize the real danger our government faces from increasingly sophisticated cyberattacks, with threats ranging from mischievous hacking incidents to serious criminal activity or highly sophisticated cyber-penetration or attacks from nation-states.

Now, while the men and women of our Federal Government are incredibly talented and dedicate and work tirelessly to leverage the resources available to them to defend our government networks, the broad challenges inherent in cybersecurity and the often cumbersome government procurement process mean that they may not always have the specific expertise or capabilities or technology necessary to keep up with current threats.

This is very sobering in light of the fact that as we know, technology itself squares every 18 months, well, particularly on the human capital side. In such cases, the private sector can offer greater flexibility and a wider ranger of specialists, as well as agility. Current law does not allow, surprisingly, for security experts to share their cybersecurity expertise and knowledge with the men and women charged with defending our Nation's critical networks and data.

So my amendment directs the Presidential cybersecurity workforce assessment provided for in the bill before us today to study the possibility of permitting temporary assignments of private sector cybersecurity professionals to Federal agencies.

Now, these assignments would offer an important opportunity for the Federal Government to tap into a wider talent pool and improve private sector involvement and cooperation in protecting our Federal networks.

By creating easier access to that expertise through temporary assignments in the Federal Government, we can dramatically improve our ability to protect the public and private cyber-infrastructure. I think this really amounts to being a real force multiplier and a benefit to the American people and our Nation as a whole.

So I urge all of my colleagues to support this noncontroversial and commonsense amendment.

I reserve the balance of my time.

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

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

There was no objection.

Mr. MCCAUL. Let me tell you it is a point of personal privilege to commend the gentleman from Rhode Island for all of his great work in this particular area and how much I have enjoyed working with the gentleman, co-chairing the CSIS commission and also co-chairing the Congressional Cybersecurity Caucus. So thank you.

This amendment would modify the section of the bill requiring the President to transmit a cybersecurity workforce report to Congress, specifically by requiring that the President's review consider the potential for temporary assignment of private sector cybersecurity professionals as a means through which to meet Federal workforce needs.

These types of mechanisms, such intergovernmental personnel agreements, have long been used by Federal agencies in various capacities; and they provide a flexible means through which to address workforce needs expeditiously.

Accordingly, it makes sense for the President's workforce assessment to consider and report on these mechanisms. So therefore, I support the gentleman's amendment.

I yield back the balance of my time.

Mr. LANGEVIN. Mr. Chair, I would just again reiterate the fact that we have some incredibly talented and dedicated men and women who work within the Federal Government already that are working day in and day out to protect what is a critical national asset, and that is our cyber-assets, as the President has clearly identified is a critical national asset and very important to our Nation's security as well as to our economy. And yet we face the incredible challenge of staying one step ahead of the bad guys, if you will, which is becoming increasingly difficult.

This amendment would basically allow us to determine a way to allow private sector involvement to a greater degree while allowing, in a sense, detailees, if you will, or temporary assignments from the private sector to Federal Government agencies that would allow us to utilize their talent, again, acting as a force multiplier to making sure that we always have the best and the brightest and we are agile at being able to use the best talents available to us to make sure that we have robust cybersecurity in protecting, as I said, this critical national asset.

So with that, I yield back the balance of my time.

The Acting CHAIR. The question is on the amendment offered by the gentleman from Rhode Island (Mr. LANGEVIN).

The amendment was agreed to.

AMENDMENT NO. 13 OFFERED BY MS. LORETTA SANCHEZ OF CALIFORNIA

The Acting CHAIR. It is now in order to consider amendment No. 13 printed in House Report 111–410.

Ms. LORETTA SANCHEZ of California. Mr. Chair, I have an amendment at the desk.

The Acting CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Amendment No. 13 offered by Ms. LORETTA SANCHEZ of California:

Page 7, line 15, insert ''representing realistic threats and vulnerabilities'' after ''event data''.

Page 23, line 2, strike ''rights and'' and insert ''rights,''.

Page 23, line 3, insert '', and for the sharing of lessons learned on the effectiveness of new technologies from the private sector with the public sector'' after ''private sector''.

The Acting CHAIR. Pursuant to House Resolution 1051, the gentlewoman from California (Ms. LORETTA SANCHEZ) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentlewoman from California.

Ms. LORETTA SANCHEZ of California. Mr. Chairman, I yield myself as much time as I may consume.

Mr. Chairman, the challenge of defending our Nation on a constantly expanding cyberfront continues to grow.

As vice chair of the House Homeland Security Committee and chairwoman of the Armed Services subcommittee that oversees the Department of Defense cybermission, I have constantly tried to improve how we address the need for the next generation technology and personnel to defend our country against this 21st-century cyberthreat.

The underlying legislation, I believe, is an important step towards enhancing our Nation's cybersecurity laws; and I have been a strong supporter of engaging the private sector in cybersecurity issues, especially when it comes to securing critical cyber-infrastructure.

To this end, the amendments that I am offering today would strengthen two existing provisions in the bill to further enhance the cybersecurity dialogue between the public and the private sectors. My amendment would add language to help facilitate access to realistic threats and vulnerabilities for our academic researchers during the development of the strategic plan that is in section 103 of the bill.

In addition, the amendment will strengthen section 108 by ensuring that the university-industry task force will propose guidelines for the private sector to provide feedback to the public sector on the effectiveness of the new technologies. This sharing of ''lessons learned'' will help us to improve critical cybersecurity technologies.

I urge my colleagues to support this amendment and the underlying legislation.

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

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

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

There was no objection.

Mr. MCCAUL. Let me say first I commend the gentlelady from California for the emphasis on the private sector.

I think too often when we deal with this issue, we focus mainly on the government and not enough on the private sector where the majority of the critical infrastructures are in this country. So let me commend the gentlelady for bringing this forward.

This amendment makes two changes to the bill which I believe are good changes. First, it requires that the cybersecurity R&D strategic plan describe how interagency efforts will facilitate access to realistic threat and vulnerability data by academic researchers. Secondly, it tasks the university-industry R&D task force created by the bill to consider how best the public and private sectors can share ''lessons learned on the effectiveness of new technologies.''

Both of these provisions make changes to the underlying bill that I believe improve the bill, and therefore I fully support its passage.

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

Ms. LORETTA SANCHEZ of California. Mr. Chairman, I yield such time as he may consume to Mr. LIPINSKI of Illinois.

Mr. LIPINSKI. Mr. Chairman, I want to commend Ms. SANCHEZ for her work on this amendment and also on cybersecurity in general on the Homeland Security Committee. From my time as a university professor, I understand the importance, first of all, of the cooperation between the private sector and universities. It is something that I feel very strongly about. We need to improve that; and certainly in cybersecurity, it is especially important.

The other thing that I understand is the need to have information, and the more information sharing that we can have, the better we can do with cybersecurity.

This amendment helps accomplish both of those things, so I strongly encourage my colleagues to support and vote for this amendment.

Ms. LORETTA SANCHEZ of California. Mr. Chairman, I believe that I have no further speakers, and therefore, I urge my colleagues to support my amendment and the underlying bill, and I yield back my time.

The Acting CHAIR. The question is on the amendment offered by the gentlewoman from California (Ms. LORETTA SANCHEZ).

The amendment was agreed to.

AMENDMENT NO. 14 OFFERED BY MR. CUELLAR

The Acting CHAIR. It is now in order to consider amendment No. 14 printed in House Report 111–410.

Mr. CUELLAR. 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:

Amendment No. 14 offered by Mr. CUELLAR:

Page 7, line 15, strike ''and''.

Page 7, line 20, strike the period and insert ''; and''.

Page 7, after line 20, insert the following new paragraph:

(7) describe how the Program will strengthen all levels of cybersecurity education and training programs to ensure an adequate, well-trained workforce.

The Acting CHAIR. Pursuant to House Resolution 1051, the gentleman from Texas (Mr. CUELLAR) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentleman from Texas.

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

First of all, Mr. Chairman, I want to rise in support of this particular amendment of the Cybersecurity Enhancement Act. I certainly want to thank Mr. LIPINSKI for all the leadership that he has provided on this bill and the staff that worked so hard. I certainly want to thank my good friend from Texas also, Mr. MCCAUL, who has worked very hard on this issue, especially on the homeland security. We appreciate your working on that, Mr. MCCAUL.

This legislation will greatly improve the cybersecurity in both the private and public sector. As any modern business, small or large, will tell you, we live in a highly interconnected, highly technological 21st century.

As a member of the Homeland Security Committee, I know that we are under attack from cyberthreats every single day. Sensitive security and intelligence information pass through the Internet 24 hours a day, 7 days a week. And more than $1 trillion was spent last year fighting to keep this information safe. The more we rely on IT systems, the more we need to make the necessary investments to reduce cyberrisks and vulnerabilities.

My amendment today is simple. As we improve cybersecurity, we must help put Americans back to work.

□ 1445

My amendment requires that the advisory committee, as it produces a cybersecurity strategic research and development plan, determine how we ought to strengthen all levels of cybersecurity education and training programs to develop a well-trained workforce that meets our Nation's cybersecurity needs. We must work to enlist our Nation's high schools, trade schools, colleges, and universities to bring more young people into this industry.

We can also use the cybersecurity education to harness the technological powers of our own young people to keep our Nation and our Nation's businesses safe. We have an opportunity to strengthen the IT infrastructure in our workforce by getting together in partnership with our Nation's schools.

In my home State of Texas, we are leaders in the cybersecurity operation. As Mr. MCCAUL understands, Texas invests in people and productive technology both in the public and private academic sectors. In San Antonio, for example, we have the National Center for Excellence for Cybersecurity, which has increased job numbers in the cybersecurity and information assurance industries in Texas. We can also replicate this particular model.

Mr. Chairman, as you know, we want to make sure that we repair our economy and help put people back to work. This is why we must strengthen our cyberinfrastructure both in business, education, and government alike. We can focus on these goals; that is, how can we secure the IT future and how do we put people back to work?

I urge all my colleagues to support this amendment.

I reserve the balance of my time.

Mr. MCCAUL. Mr. Chairman, I rise to claim time in opposition to this amendment. However, the good news is, Mr. CUELLAR, I do not intend to oppose it.

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

There was no objection.

Mr. MCCAUL. Let me first commend the gentleman from Texas, my dear friend and colleague, Mr. CUELLAR, on the outstanding work he has done in this area and on the Homeland Security Committee, and also his work with the Center for Excellence, in San Antonio, for cybersecurity. It is great for our great State of Texas.

This amendment requires a strategic plan to describe how the program will strengthen cybersecurity education and training efforts in order to ensure an adequate, well-trained workforce. The bill already has in place a robust workforce assessment requirement, but the robustness of our future cybersecurity workforce I believe is important enough to reemphasize it.

With that, I do not oppose this amendment. In fact, I strongly support it.

I yield back the balance of my time.

Mr. CUELLAR. Mr. Chairman, I just want to echo Mr. MCCAUL's words on this, that we need to make sure that we support our business, both public and private. I think this amendment will accomplish that, especially working with our education.

Again, to the chairman, thank you very much, and to the staff who worked so hard on this.

I ask Members to support this particular amendment.

I yield back the balance of my time.

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

The question was taken; and the Acting Chair announced that the ayes appeared to have it.

Mr. CUELLAR. Mr. Chair, I demand a recorded vote.

The Acting CHAIR. Pursuant to clause 6 of rule XVIII, further proceedings on the amendment offered by the gentleman from Texas will be postponed.

AMENDMENT NO. 15 OFFERED BY MS. SHEA-PORTER

The Acting CHAIR. It is now in order to consider amendment No. 15 printed in House Report 111–410.

Ms. SHEA-PORTER. I have an amendment at the desk.

The Acting CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Amendment No. 15 offered by Ms. SHEA-PORTER:

Page 15, line 11, strike ''equal to the length of the scholarship'' and insert ''as provided in paragraph (5)''.

Page 15, after line 24, insert the following new paragraph:

(5) LENGTH OF SERVICE.—The length of service required in exchange for a scholarship under this subsection shall be as follows:

(A) For a recipient in a bachelor's degree program, 1 year more than the number of years for which the scholarship was received.

(B) For a recipient in a Master's degree program, 2 years more than the number of years for which the scholarship was received.

(C) For a recipient in a doctorate degree program, 3 years more than the number of years for which the scholarship was received.

The Acting CHAIR. Pursuant to House Resolution 1051, the gentlewoman from New Hampshire (Ms. SHEA-PORTER) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentlewoman from New Hampshire.

Ms. SHEA-PORTER. Mr. Chairman, I yield myself such time as I may consume.

I would like to thank Chairman GORDON for his hard work on this bill. As a member of the House Armed Services Committee, I know just how important it is that we focus on cybersecurity and combating the threats that we face. It is an incredibly important area, and I commend him for his work.

Mr. Chair, as cyberattacks become increasingly common and alarming, the government needs more expert cybersecurity personnel to protect us. The Scholarships for Service program is an important means to recruit such expert personnel. However, I believe that considering the high value of the education and security clearance, which is all provided at government expense, the current service obligation is insufficient to recover the significant Federal investment we are making.

My amendment extends the service obligation for recipients of cybersecurity scholarships or fellowships on a sliding scale depending on the degree program. Those in bachelor's degree programs would see their service requirement extend by 1 year to 3 years, those in a master's program by 2 years to 4 years, and those in a Ph.D. program by 3 years to 5 or 6 years, depending on the program.

Graduate students in cybersecurity programs need to have security clearances, and most students will need a clearance before beginning work in this field for the Federal Government. The cost of a clearance, which is a pricey $15,000, is an investment by the taxpayers and should be recovered by the Federal Government through an extension of service.

Extending the work requirement will also help slow the revolving door from government to industry and promote retention of valuable employees. Because these employees will have a security clearance, which is generally good for 10 years, they may be tempted to take their expertise into the private sector where they can make higher salaries. This amendment will help ensure recruitment of those who want to serve in the government and will prevent this valuable program from being used solely as a bridge to private industry.

It is fair to scale the extra work commitment according to degree, because a graduate degree with a clearance is far more valuable than an undergraduate degree with a clearance. The longer the educational investment, the longer the service requirement should be. A Ph.D. graduate should serve longer than a master's graduate who should serve longer than a bachelor's graduate. The extension of service allows us to retain those we train at government expense for a longer time, leading to a positive impact on retention and on our cybersecurity.

My amendment will increase retention of our valuable personnel who are trained at taxpayer expense. It is a good deal for the government and the student and represents a wise use of taxpayer funds.

I urge my colleagues to support this amendment.

I reserve the balance of my time.

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

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

There was no objection.

Mr. MCCAUL. The gentlelady from New Hampshire's amendment is one that our side favored during the drafting of this legislation and one that we think makes the Scholarship for Service program at NSF even stronger. So I thank the gentlelady for bringing this amendment.

The intent of the program is to educate the Federal Government's future cybersecurity workforce. This amendment increases the amount of employment service a graduate will owe the Federal Government upon the completion of her or his education, ensuring a greater return on our initial investment.

Therefore, I support this amendment, and I encourage my colleagues to do so.

I yield back the balance of my time.

Ms. SHEA-PORTER. I yield to the chairman, the gentleman from Illinois (Mr. LIPINSKI) such time as he may consume.

Mr. LIPINSKI. Mr. Chairman, I want to thank the gentlelady from New Hampshire for her amendment. It certainly ensures that we retain individuals who are trained at government expense, making sure the Scholarship for Service program provides the best value for taxpayers, and it is certainly also a good value for those who are receiving their education. It is a good, commonsense amendment, and I urge my colleagues to support it.

Ms. SHEA-PORTER. I thank the chairman and his staff for the work on this bill. I urge my colleagues to support this amendment and the underlying bill.

I yield back the balance of my time.

The Acting CHAIR. The question is on the amendment offered by the gentlewoman from New Hampshire (Ms. SHEA-PORTER).

The amendment was agreed to.

AMENDMENT NO. 16 OFFERED BY MS. CLARKE

The Acting CHAIR. It is now in order to consider amendment No. 16 printed in House Report 111–410.

Ms. CLARKE. Mr. Chairman, I rise to address the floor on my amendment.

The Acting CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Amendment No. 16 offered by Ms. CLARKE:

Page 20, line 24, insert ''the extent to which different agencies and departments rely on contractors to support the Federal cybersecurity workforce,'' after ''agencies and departments,''.

Page 21, line 22, strike ''and''.

Page 21, line 23, redesignate paragraph (5) as paragraph (6).

Page 21, after line 22, insert the following:

(5) a specific analysis of the capacity of the agency workforce to manage contractors who are performing cybersecurity work on behalf of the Federal Government; and

The Acting CHAIR. Pursuant to House Resolution 1051, the gentlewoman from New York (Ms. CLARKE) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentlewoman from New York.

Ms. CLARKE. Mr. Chairman, today I rise to offer my amendment to H.R. 4061 and request that it be supported along with the underlying legislation.

I first want to commend Chairman GORDON, Ranking Member HALL, and Representative LIPINSKI, as well as Representative MCCAUL, for their leadership in bringing this important bipartisan bill to the floor today and for supporting this amendment.

The Federal Government currently relies heavily on contract employees for critical cybersecurity functions. For instance, according to the Department of Homeland Security's Inspector General, contractors accounted for 83 percent of the total staff of the Department's Office of the Chief Information Officer.

A July 2009 Booz Allen Hamilton assessment of the cyberworkforce, titled, ''Cyber In-Security: Strengthening the Federal Cybersecurity Workforce,'' concluded the Federal Government needs more employees who can effectively manage the blended cybersecurity workforce of contractors and in-house employees.

Clearly, any assessment of the cybersecurity workforce should include an analysis of contract employees who perform cybersecurity functions for the government. My amendment to H.R. 4061, the Cybersecurity Enhancement Act of 2009, would do just that, amending section 107 of the bill to include an

analysis of the extent to which Federal agencies rely on contractors to support the Federal cybersecurity workforce as well as each agency's capacity to manage these contractors.

The amendment is not intended to judge whether Federal cybersecurity functions should be performed by government or contractor employees. It simply requires that these considerations be included in the workforce study.

I hope that you will join me in supporting this amendment.

I would just like to add that, as chair of the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, I have become intimately aware of the cybersecurity challenges we face in the 21st century. I initially offered several other amendments which address the wide variety of challenges that we face, and I will work to address these issues through my subcommittee.

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

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

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

There was no objection.

Mr. MCCAUL. Let me first commend Ms. CLARKE for this amendment, but also her great work on the Homeland Security Committee as the chairwoman of the Cybersecurity Subcommittee.

This amendment simply requires the present Cybersecurity Workforce Assessment Report include an analysis of the capacity of the overall agency workforce to manage contractors providing cybersecurity support to Federal agencies. Contractors are a significant component of our cybersecurity efforts, and assessing their role and agencies' capacity to manage them is very, very appropriate. Therefore, I support this amendment.

With the time I do have remaining, Mr. Chairman, I would like to yield to the gentlelady from Texas, Ms. SHEILA JACKSON LEE.

Ms. JACKSON LEE of Texas. I thank the distinguished gentleman, and I thank him for his leadership on homeland security as well and as ranking member positioned on the Cybersecurity Committee. And I thank the chairwoman of the Cybersecurity Committee, and I thank her for this amendment which I rise to support.

I am the chairwoman of the Subcommittee on Transportation Security and Infrastructure Protection. There is a great deal of overlap. So I thank Mr. LIPINSKI, Mr. EHLERS, Mr. WU, Mr. SMITH, Mr. HALL.

We have been fortunate as to not have a major catastrophic incident with cybersecurity, but this bill will help ensure a strategic plan for Federal cybersecurity research and development, strengthen public-private partnerships in cybersecurity, and help train the next generation of cybersecurity professionals and improve cybersecurity technical standards.

Ms. CLARKE's amendment is a very vital amendment, for it will help subject to the assessment of the President's committee the same assessment on employees. This will assess the contractors who are dealing with cybersecurity, including minority women and small contractors of which we hope will increase.

While we have been fortunate so far in avoiding a catastrophic cyberattack, last year the Pentagon reported more than 360 million attempts to break into its networks. A 2009 Consumer Reports study found that, over the past 2 years, one in five online consumers had been a victim of cybercrime. In 2008, the Department of Homeland Security logged 5,499 such cyberattack incidents, a 40 percent increase over the previous year. A 2007 Government Accountability Office report estimates that total U.S. business losses due to cyberattacks exceed $117.5 billion per year.

This amendment will also put under scrutiny those contractors that are working in cybersecurity for the Federal Government, along with those employees. We have to be diligent in, one, making sure that this is a, if you will, securer technology that is being used around the country and around the world, but we must also be diligent in increasing the R&D and making sure that contractors are adhering to the rules and guidelines that are equal to excellence, as we want our employees.

Let me ask my colleagues to support the underlying bill and this amendment, and as well to be reminded that this is part of the Nation's homeland security.

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

Ms. CLARKE. I yield such time as he may consume to the gentleman from Illinois (Mr. LIPINSKI).

Mr. LIPINSKI. This is a very good and thoughtful amendment, and I thank Ms. CLARKE for helping to ensure that the Federal workforce assessment that we require in our report is complete and thorough in its analysis. I would like to also thank Ms. CLARKE and her staff for working with the committee on this language, and I strongly support this amendment and urge my colleagues to vote for it.

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

The Acting CHAIR. The question is on the amendment offered by the gentlewoman from New York (Ms. CLARKE).

The amendment was agreed to.

□ 1500

AMENDMENT NO. 17 OFFERED BY MR. BRIGHT

The Acting CHAIR. It is now in order to consider amendment No. 17 printed in House Report 111–410.

Mr. BRIGHT. 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:

Amendment No. 17 offered by Mr. BRIGHT:

Page 27, after line 7, insert the following new section:

SEC. 111. NATIONAL ACADEMY OF SCIENCES STUDY ON THE ROLE OF COMMUNITY COLLEGES IN CYBERSECURITY EDUCATION.

Not later than 120 days after the date of enactment of this Act, the Director of the Office of Science and Technology Policy, in consultation with the Director of the National Coordination Office, shall enter into a contract with the National Academy of Sciences to conduct and complete a study to describe the role of community colleges in cybersecurity education and to identify exemplary practices and partnerships related to cybersecurity education between community colleges and four-year educational institutions.

The Acting CHAIR. Pursuant to House Resolution 1051, the gentleman from Alabama (Mr. BRIGHT) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentleman from Alabama.

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

Mr. Chairman, I rise today in support of my amendment to the Cybersecurity Enhancement Act, H.R. 4061. Put simply, this amendment would require the National Academy of Sciences to conduct a study on the role of community colleges in cybersecurity education. It would also identify best practices related to cybersecurity education between community colleges and 4-year educational institutions.

By now, we all recognize the need for the underlying legislation. It was made even more evident following the State of the Union last week, when numerous congressional Web sites, including mine, were hacked by foreign actors. Without a doubt, we need to improve our national cybersecurity infrastructure. As the United States transitions into a future which addresses such cybersecurity issues, it will become increasingly important that we adopt advanced job skills and technological savvy. Unfortunately, a high school diploma is often not enough to qualify for the jobs of tomorrow. Recognizing the need for additional education, workers often return to technical schools and community colleges to obtain advanced training.

My amendment will serve to strengthen the community colleges that already play an important role in many of our districts. As demand for a skilled cybersecurity workforce continues to rise, we must be ready to supply it. This amendment will ensure that community colleges will play a role in providing these personnel that will be needed in the future.

This amendment is also consistent with the President's vision for promoting post-secondary education. In his State of the Union address to Congress last week, President Obama called for every American to commit to at least 1 year or more of higher education or career training. Some of

that training will happen in community college classrooms. This amendment could expand the options available in those classrooms across the country and make it easier for our constituents to commit to our shared goal of increased higher education.

As I worked my way through college when I was growing up, I began at the local Enterprise State Community College, which is located in my district. So I understand the value of 2-year institutions. My district alone is home to seven different community and technical colleges. And many Members of Congress are committed to preserving and protecting their role in our educational system. As we transition into 21st century jobs, it is vital that we also provide the resources to our community colleges that would allow them to change with the times. The amendment achieves that goal.

Mr. Chairman, this amendment is simple and straightforward. It ensures a level playing field for community colleges wishing to offer educational opportunities in the cybersecurity field, and improves information sharing between 2-year and 4-year colleges. I urge its passage today.

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

Mr. MCCAUL. Mr. Chairman, I claim time in opposition to this amendment, although I am not opposed to it.

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

There was no objection.

Mr. MCCAUL. This amendment would require a National Academy of Sciences study on the role of community colleges in cybersecurity education, with an aim toward identifying best practices related to improving cybersecurity education through better linkages between community colleges and 4-year colleges and universities. It is important not to overlook the contributions of community colleges, as the gentleman stated, to our overall technical workforce, including those involved in computer and network security. This amendment is intended to help address that issue, and I strongly urge my colleagues to support it.

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

Mr. BRIGHT. In closing, I would like to thank Chairman GORDON and his staff on the Science and Technology Committee for their attention to this issue and for working with my staff to draft this amendment. I would also like to thank Chairwoman SLAUGHTER and the Rules Committee for helping my staff put this together and allowing me to offer this amendment today on the floor.

Again, I urge all my colleagues today to support my amendment.

I yield back the remainder of my time.

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

The amendment was agreed to.

AMENDMENT NO. 18 OFFERED BY MR. CONNOLLY OF VIRGINIA

The Acting CHAIR. It is now in order to consider amendment No. 18 printed in House Report 111–410.

Mr. CONNOLLY of Virginia. 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:

Amendment No. 18 offered by Mr. CONNOLLY of Virginia:

Page 28, line 12, insert ‘‘, including among children and young adults,’’ after ‘‘public awareness’’.

The Acting CHAIR. Pursuant to House Resolution 1051, the gentleman from Virginia (Mr. CONNOLLY) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentleman from Virginia.

Mr. CONNOLLY of Virginia. I thank the Chair, and I yield myself such time as I may consume.

First of all, let me thank, Mr. Chairman, the leadership of Chairman GORDON and Ranking Member HALL and the floor managers, Mr. LIPINSKI of Illinois and Mr. MCCAUL of Texas. I appreciate very much their leadership.

Cybersecurity, Mr. Chairman, has been a growing concern, and recent events like the attack on Google and the hacking of Web sites maintained by Members of this very Chamber in the House highlight the urgency of today's action. As you know, the bill would expand research and development work in the field of cybersecurity, to provide for increased higher education opportunities, and to launch a much needed public awareness campaign on the importance of making our electronic communications and commerce as secure as possible in today's digital age.

My amendment, Mr. Chairman, would clarify that children and young adults should be an important target audience of that public awareness campaign, and must be included. Children and young adults are by far among the largest consumers of new media and technology, yet in many cases they are also the most naive when it comes to taking basic safety precautions when using this technology and these innovations, which makes it all the more important that we reach out to them specifically.

While children and young adults are among the most savvy users of technology, I fear they do not fully grasp the permanence of their actions, whether it is blogging, Facebooking, Tweeting, or posting videos on YouTube. The use and portability of information technology has exploded in the past decade. More than 80 percent of households, for example, in my district have Internet access. Technology has become a vital part of our everyday lives, particularly for the younger generation.

According to the Center for Education Statistics, 67 percent of preschool children have used a computer, and 23 percent of preschool children have used the Internet. Those figures of course jump exponentially higher once children reach school age, as technology becomes integrated into the classroom curriculum. By the time young people reach high school, 97 percent of them are using computers, and 80 percent are online regularly, which for parents of teenagers like myself, that may sound like a conservative figure.

I cannot emphasize enough, Mr. Chairman, how important it is for us to reach children at a young age, in the classroom, to develop a healthy sense of caution as we instruct them about the wonders of technology. That is particularly true in our science, technology, engineering and math-focused schools.

That is why in my district, Thomas Jefferson High School, ranked the number one high school in the United States 3 years in a row, is churning out the innovators of tomorrow. I look forward to exploring future opportunities in this area with the committee and urge my colleagues to support this important legislation.

With that, I reserve the balance of my time.

Mr. MCCAUL. Mr. Chairman, I claim time in opposition to this amendment, although I am not opposed to it.

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

There was no objection.

Mr. MCCAUL. First let me say what a great amendment this is. As a Federal prosecutor, I encountered crimes against children and also as deputy attorney general for the State of Texas. While there, we formed an Internet crimes against children's task force. The threat to children, both from child pornography and online predators, as the gentleman knows, is very real. And while the Internet is a great tool for our youth, it also does present a vulnerability and a threat to them. That is why I am so glad to see this amendment.

It simply clarifies when we are promoting and educating people on the importance of cybersecurity, we must include children and young adults along with the other targeted audiences. So let me again thank the gentleman for bringing this. I strongly support it, and encourage my colleagues to do so.

I yield back the balance of my time.

Mr. CONNOLLY of Virginia. I yield to the gentleman from Illinois, the distinguished floor manager.

Mr. LIPINSKI. I want to commend the gentleman from Virginia for his amendment. Obviously, as the gentleman talked about, the Internet is great for children, young adults, provides so many opportunities, but we need to be very careful because we all know the dark side and the down side. So much more can be done and should be done to protect children, young

adults. And Mr. CONNOLLY's amendment does that. So I want to urge my colleagues to support the amendment.

Mr. CONNOLLY of Virginia. I thank my distinguished colleagues, Mr. Chairman, and I yield back the balance of my time.

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

The question was taken; and the Acting Chair announced that the ayes appeared to have it.

Mr. CONNOLLY of Virginia. Mr. Chairman, I demand a recorded vote.

The Acting CHAIR. Pursuant to clause 6 of rule XVIII, further proceedings on the amendment offered by the gentleman from Virginia will be postponed.

AMENDMENT NO. 19 OFFERED BY MRS. HALVORSON

The Acting CHAIR. It is now in order to consider amendment No. 19 printed in House Report 111–410.

Mrs. HALVORSON. 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:

Amendment No. 19 offered by Mrs. HALVORSON:

Page 15, line 2, strike ''need and to'' and insert ''need, to''.

Page 15, line 5, insert before the period at the end of paragraph (2) '', and to veterans. For purposes of this paragraph, the term ''veteran'' means a person who—

(A) served on active duty (other than active duty for training) in the Armed Forces of the United States for a period of more than 180 consecutive days, and who was discharged or released therefrom under conditions other than dishonorable; or

(B) served on active duty (other than active duty for training) in the Armed Forces of the United States and was discharged or released from such service for a service-connected disability before serving 180 consecutive days.

For purposes of subparagraph (B), the term ''service-connected'' has the meaning given such term under section 101 of title 38, United States Code.

The Acting CHAIR. Pursuant to House Resolution 1051, the gentlewoman from Illinois (Mrs. HALVORSON) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentlewoman from Illinois.

Mrs. HALVORSON. Mr. Chairman, I yield myself as much time as I may consume.

I rise to urge my colleagues to support my amendment to H.R. 4061, the Cybersecurity Enhancement Act of 2009. This amendment is simple, necessary, and beneficial to veterans. It will add veteran status as an additional item of consideration when selecting individuals for the Cyber Scholarship for Service program.

In light of recent attacks on both government and commercial technology infrastructure, it is critical that America be on the forefront of cybersecurity. Our veterans and servicemembers have a proven track record of successfully protecting American interests at home and abroad. The experiences and skills that our veterans have gained through their service are exactly what we need to improve our cybersecurity.

My amendment helps veterans continue their service to our country by increasing the likelihood that a veteran or servicemember will be selected for this competitive scholarship. The scholarship program will provide funding to individuals seeking B.A.s, M.A.s, and Ph.D.s in the field of cybersecurity. This amendment will allow our veterans and servicemembers to afford a better education and continue to serve their country.

Additionally, many veterans and servicemembers have already received cybersecurity and other relevant training during their service in the military. They are uniquely qualified to defend our Nation from cybersecurity threats we face. Furthermore, upon successful completion of their degree, scholarship recipients will be eligible for Federal employment in the field of cybersecurity. With thousands of veterans returning from service in Iraq and Afghanistan, and more than 20 percent of veterans under the age of 24 unemployed, it is critical that they are given every opportunity to continue serving their country.

Our veterans and servicemembers have sacrificed to protect our country and our freedom. We owe them all the assistance we can give them in helping them to better education and job opportunities in their civilian lives.

I would like to thank the committee and the chairman for working with my colleague from New Hampshire and me to introduce this amendment. Once again, I rise in strong support of the amendment, and I urge my colleagues to vote in support of it.

With that, I reserve the balance of my time.

Mr. MCCAUL. Mr. Chairman, I claim time in opposition to this amendment, although I am not opposed to it.

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

There was no objection.

Mr. MCCAUL. Let me thank the gentlelady for bringing this amendment. My home State of Texas is the home to probably more active duty service and veterans than probably any other State in the country. I think this is a great idea, including Lackland Air Force Base, which provides a cybersecurity command.

It is very straightforward. It adds veteran status as an additional item for consideration by NSF when it selects individuals for scholarships under its Cybersecurity Scholarships for Service program. Therefore, I strongly support the gentlelady's amendment, and I urge its passage.

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

□ 1515

Mrs. HALVORSON. With that, I yield 1 minute to my colleague, the gentlewoman from New Hampshire (Ms. SHEA-PORTER).

Ms. SHEA-PORTER. I was proud to work with my colleague, Representative DEBBIE HALVORSON, on this amendment. It is critical that we ensure every opportunity for our veterans who have served our country so admirably. This commonsense amendment makes sure their service is taken into consideration when being selected for the Federal Cyber Service Scholarship for Service. As a member of the Armed Services Committee, I understand how critical it is that we defend against cyberattacks. That means that we need a workforce dedicated to protecting our country. Our men and women who have volunteered in our armed services have showed exceptional courage and dedication. That service should always be met with our gratitude and our support. This amendment ensures that when someone has served our country, we give that service due consideration when they ask to serve again.

I thank my colleague for offering this amendment, and I urge my colleagues to support it.

Mrs. HALVORSON. I yield the remainder of my time to the gentleman from Illinois (Mr. LIPINSKI).

Mr. LIPINSKI. I'd like to thank Mrs. HALVORSON and Ms. SHEA-PORTER for their amendment and more broadly for all the work that they do on behalf of our veterans. It certainly is an issue of great importance. Last night, I had a father come to me and tell me that his son had come back from Iraq and was having trouble finding a job and was actually faced with re-enlisting because of his struggles in trying to find something. This amendment will certainly help there. Many of our veterans have technical backgrounds already. With some additional training, they are well positioned to continue serving their country by joining our Federal cybersecurity workforce, including at civilian agencies.

So I want to, again, commend Mrs. HALVORSON for her amendment, and strongly urge my colleagues to support it.

Mrs. HALVORSON. In closing, I just urge my colleagues to vote ''yes,'' and I yield back the balance of my time.

The Acting CHAIR. The question is on the amendment offered by the gentlewoman from Illinois (Mrs. HALVORSON).

The question was taken; and the Acting Chair announced that the ayes appeared to have it.

Mrs. HALVORSON. Mr. Chair, I demand a recorded vote.

The Acting CHAIR. Pursuant to clause 6 of rule XVIII, further proceedings on the amendment offered by the gentlewoman from Illinois will be postponed.

AMENDMENT NO. 20 OFFERED BY MS. KILROY

The Acting CHAIR. It is now in order to consider amendment No. 20 printed in House Report 111–410.

Ms. KILROY. 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:

Amendment No. 20 offered by Ms. KILROY:
Page 14, line 10, strike ''and''.
Page 14, line 12, strike the period and insert ''; and''.
Page 14, after line 12, insert the following new subparagraph:
(D) outreach to secondary schools and 2-year institutions to increase the interest and recruitment of students into cybersecurity-related fields.

The Acting CHAIR. Pursuant to House Resolution 1051, the gentlewoman from Ohio (Ms. KILROY) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentlewoman from Ohio.

Ms. KILROY. I yield myself such time as I may consume. I rise today in support of my amendment to H.R. 4061, the Cybersecurity Enhancement Act of 2009, to expand outreach to high school and community colleges to help train and recruit the next generation of our Nation's cybersecurity and information technology workforce. One of the most important aspects of the Cybersecurity Enhancement Act is the establishment of the Scholarship for Service program currently administered by the National Science Foundation. The program would operate with the goal of recruiting and training our Nation's future cybersecurity professionals through scholarships for undergraduate and graduate students in cybersecurity fields, government internship opportunities for scholarship recipients, and competitive, merit-based grants for faculty development, institutional partnerships, and the development of cybersecurity courses at institutions of higher learning.

My amendment will expand the Scholarship for Service program by making merit-based grants available for outreach to high schools and community colleges. Reaching out to high schools will help raise awareness of this program, steering students at an earlier age toward academic and professional careers in information technology and cybersecurity that they might not otherwise have considered. Young people are way ahead of us in terms of information technology and the use of computers but they still need the encouragement and guidance to pursue a cybersecurity career path. That guidance can be made possible through these kind of competitive grants.

My amendment also will expand outreach to community colleges. Cybercriminals are increasingly targeting small businesses, schools, and State and local institutions that lack the capabilities to adequately defend themselves against sophisticated cyberattacks. Encouraging students at community colleges to consider degrees in cybersecurity-related fields will help ensure that we have a workforce capable of defending our Nation's computer systems and networks at the State, local, and national level.

As a member of the Homeland Security Committee's Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, I strongly support the efforts of H.R. 4061 to build our Nation's cybersecurity workforce, develop a strategic research plan for cybersecurity, and to secure our communications and information technology infrastructure.

I reserve the balance of my time.

Mr. MCCAUL. Mr. Chairman, I rise to claim time in opposition to this amendment, although I do not intend to oppose it.

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

There was no objection.

Mr. MCCAUL. I thank the gentlelady for this amendment. Certainly, our youth know the Internet and how to operate on it more effectively than anyone in this Chamber. This amendment adds an outreach to high schools and community colleges component to the characteristics of the Scholarship for Service program in an effort to attract more students to the program. I think it's a good idea. I support this amendment, and urge my colleagues to do so.

I yield back the balance of my time.

Ms. KILROY. I thank my colleague from Texas, who also serves with me on the Homeland Security Committee. I want to commend Chairman GORDON; Ranking Member HALL; Subcommittee Chair LIPINSKI, the sponsor of this legislation; and the Committee on Science and Technology for their hard work on H.R. 4061, to help build a strong cybersecurity workforce to protect and serve our Nation's communications and IT infrastructure. I look forward to continuing to work with my colleagues to ensure that the Nation's essential infrastructure is protected, and I urge my colleagues to support my amendment expanding cybersecurity outreach to high schools and community colleges as part of the Scholarship for Service program.

I yield back the balance of my time.

The Acting CHAIR. The question is on the amendment offered by the gentlewoman from Ohio (Ms. KILROY).

The question was taken; and the Acting Chair announced that the ayes appeared to have it.

Ms. KILROY. Mr. Chair, I demand a recorded vote.

The Acting CHAIR. Pursuant to clause 6 of rule XVIII, further proceedings on the amendment offered by the gentlewoman from Ohio will be postponed.

AMENDMENT NO. 21 OFFERED BY MR. KISSELL

The Acting CHAIR. It is now in order to consider amendment No. 21 printed in House Report 111–410.

Mr. KISSELL. 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:

Amendment No. 21 offered by Mr. KISSELL:
Page 11, lines 9 and 10, strike ''Section 5(a)(6) of such Act (15 U.S.C. 7404(a)(6)) is amended to read as follows:'' and insert ''Section 5(a) of such Act (15 U.S.C. 7404(a)) is amended—
(1) in paragraph (3)(A), by inserting '', including curriculum on the principles and techniques of designing secure software'' after ''network security''; and
(2) by amending paragraph (6) to read as follows:

The Acting CHAIR. Pursuant to House Resolution 1051, the gentleman from North Carolina (Mr. KISSELL) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentleman from North Carolina.

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

Mr. Chairman, this is a simple amendment. It highlights the importance of curriculum in designing secure software. I would like to start out also by commending the chairman and ranking member for bringing this very timely and important piece of legislation to our attention. In North Carolina, we have many institutions, as there are across the United States, that are dependent upon secure software and informing our networks that are used in such a vital part of performing business on a day-to-day basis. Whether it's in our part of the world, it's the military, banking giants of America, education, or just corporations or businesses in general, or whatever, we're dependent upon networks and software for, once again, our day-to-day operations. However, Mr. Chairman, all too often we find that these networks are not as secure as they need to be.

A recent study done by Dr. William Chu, who is the department Chair at the University of North Carolina in Charlotte, which is a leading institution on secure software issues, Dr. Chu found that 97 percent—and he did this on a random basis—they looked at corporate Web sites. And on a random basis they looked to see if the security of those networks was sufficient to keep them from being compromised, and they found that they weren't. Ninety-seven percent of the time they weren't sufficiently secure to prevent this ability for hackers to compromise.

This is a wake-up call for us. So many of these amendments and this bill address that we've got issues here, and one of the ways that we can address these issues—it is in broad agreement—is that we need to improve the curriculum of our secure software. Now we would think this would be easily done in our colleges and universities. But, unfortunately, we find that this curriculum is not taught that consistently to a large degree to allow the programmers of tomorrow to learn how to secure software.

So this amendment is very simple. It instructs the director of NSF to put language into the mission statement of Computer and Network Security Capacity Building Grants language that would highlight the importance of curriculum in designing secure software.

I reserve the balance of my time.

Mr. MCCAUL. Mr. Chairman, I rise to claim time in opposition to the amendment, but I do not intend to oppose it.

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

There was no objection.

Mr. MCCAUL. This amendment simply clarifies that NSF's support for cybersecurity-related curriculum development at universities includes ''curriculum on the principles and techniques of designing secure software.'' It's a good amendment that codifies and clarifies NSF's role in support of computer security curriculum development. I support this amendment. I urge my colleagues to do so.

I yield back the balance of my time.

Mr. KISSELL. Mr. Chair, this is a first step towards allowing our universities and colleges to be able to produce, once again, programmers of tomorrow to understand the importance of securing the software and the networks that are so important to us in so many ways. It's a first step; it is not the last step. But I do encourage my colleagues to support this and vote ''yes'' for this amendment.

I yield back the balance of my time.

The Acting CHAIR. The question is on the amendment offered by the gentleman from North Carolina (Mr. KISSELL).

The question was taken; and the Acting Chair announced that the ayes appeared to have it.

Mr. KISSELL. Mr. Chair, I demand a recorded vote.

The Acting CHAIR. Pursuant to clause 6 of rule XVIII, further proceedings on the amendment offered by the gentleman from North Carolina will be postponed.

AMENDMENT NO. 22 OFFERED BY MR. KRATOVIL

The Acting CHAIR. It is now in order to consider amendment No. 22 printed in House Report 111–410.

Mr. KRATOVIL. 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:

Amendment No. 22 offered by Mr. KRATOVIL:

Page 27, after line 7, insert the following new section:

SEC. 111. NATIONAL CENTER OF EXCELLENCE FOR CYBERSECURITY.

(a) IN GENERAL.—As part of the Program, the Director of the National Science Foundation shall, in coordination with other Federal agencies participating in the Program, establish a National Center of Excellence for Cybersecurity.

(b) MERIT REVIEW.—The National Center of Excellence for Cybersecurity shall be awarded on a merit-reviewed, competitive basis.

(c) ACTIVITIES SUPPORTED.—The National Center of Excellence for Cybersecurity shall—

(1) involve institutions of higher education or national laboratories and other partners, which may include States and industry;

(2) make use of existing expertise in cybersecurity;

(3) interact and collaborate with Computer and Network Security Research Centers to foster the exchange of technical information and best practices;

(4) perform research to support the development of technologies for testing hardware and software products to validate operational readiness and certify stated security levels;

(5) coordinate cybersecurity education and training opportunities nationally;

(6) enhance technology transfer and commercialization that promote cybersecurity innovation; and

(7) perform research on cybersecurity social and behavioral factors, including human-computer interactions, usability, user motivations, and organizational cultures.

The Acting CHAIR. Pursuant to House Resolution 1051, the gentleman from Maryland (Mr. KRATOVIL) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentleman from Maryland.

Mr. KRATOVIL. I yield myself such time as I may consume.

Mr. Chairman, let me begin by thanking Mr. GORDON, the chairman, and the ranking member for bringing the legislation to the floor. I rise in support of my amendment to the Cybersecurity Enhancement Act of 2009. Information technology has improved everything from the way we pay our bills to the way we communicate with our friends and neighbors. We are increasingly becoming a digital Nation where the strength and vitality of our economy, infrastructure, public safety, and national security are becoming more and more reliant on cyberspace. Of course, with that reliance on technology, as many have mentioned here today, come real concerns about the security of information traveling through cyberspace.

It's time we make every effort to secure and protect the privacy, finances, and resources of Americans who utilize information technology. I believe the underlying bill does much to accomplish this.

Mr. Chairman, I'm sure it won't surprise you, but I do believe that my amendment will enhance this bill by enhancing communication, collaboration, and cooperation between the public and private sectors. The amendment does so by requiring the director of the National Science Foundation to establish a National Center of Excellence for Cybersecurity. This Center would be awarded on a merit-based, comprehensive basis and would support the initiatives put forth by the underlying legislation to ensure the safety of our digital communications infrastructure. This National Center would be a partnership model involving government, private corporations, and academic institutions that will consolidate and coordinate our national cybersecurity resources.

□ 1530

As the cybersecurity industry grows, there is an increasing demand for skilled workers and a severe shortage of workers qualified to fill these jobs. The center will serve not only as a clearinghouse for our national cybersecurity resources, but it will create jobs and train individuals in the skills needed to protect the economy, bolster our national security, and protect Americans from cybercriminals.

Mr. Chairman, I want to take a brief moment also to express my support for an amendment that was heard previously, offered by Representative MCCARTHY, that would emphasize education and awareness programs in cybersecurity for populations in areas of planned broadband expansion or deployment, such as areas like my district in Maryland's Eastern Shore. Mr. Chairman, I ask my colleagues to support both amendments and the underlying bill.

I reserve the balance of my time.

Mr. MCCAUL. Mr. Chairman, I rise to claim time in opposition to this amendment, although I am not opposed.

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

There was no objection.

Mr. MCCAUL. While the statute that we are amending today already authorizes the director of NSF to provide grants for computer and network security research centers, I believe that the establishment of a National Center of Excellence dedicated solely to cybersecurity can only increase our defensive capabilities, provided that any funding that does go to the National Center does not come at the expense of other Centers of Excellence, of course. With that, I urge my colleagues' support for this amendment.

I yield back the balance of my time.

Mr. KRATOVIL. Mr. Chairman, I yield so much time as he may consume to the gentleman from Illinois (Mr. LIPINSKI).

Mr. LIPINSKI. First off, I want to commend Mr. KRATOVIL for his amendment. We have certainly seen Centers for Excellence do some very good work not only in the science and technology field, but I also know that in the transportation field, we have also seen that. I think this amendment that would establish a merit-based and a competitive-based Center for Excellence for Cybersecurity will be a great addition to our IT research in the country. I think it could be a very good enhancement to this bill, so I strongly support this amendment. I urge my colleagues to vote for this amendment.

Mr. KRATOVIL. I want to thank the gentleman from Texas for his support and also the gentleman from Illinois.

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

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

The amendment was agreed to.

AMENDMENT NO. 23 OFFERED BY MR. LIPINSKI

The Acting CHAIR. It is now in order to consider amendment No. 23 printed in House Report 111–410.

Mr. LIPINSKI. As the designee of the gentleman from Virginia, I rise to offer the amendment.

The Acting CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Amendment No. 23 offered by Mr. LIPINSKI:

Page 27, after line 7, insert the following new section:

SEC. 111. CYBERSECURITY INFRASTRUCTURE REPORT.

Not later than 1 year after the date of enactment of this Act, the Comptroller General shall transmit to the Congress a report examining key weaknesses within the current cybersecurity infrastructure, along with recommendations on how to address such weaknesses in the future and on the technology that is needed to do so.

The Acting CHAIR. Pursuant to House Resolution 1051, the gentleman from Illinois (Mr. LIPINSKI) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentleman from Illinois.

Mr. LIPINSKI. Mr. Chairman, Mr. NYE's amendment calls on the GAO to examine key weaknesses within the Nation's cybersecurity infrastructure and to offer recommendations on how the Federal Government should address those weaknesses, and calling on the GAO will help to find those areas that are especially insecure. We certainly have heard enough times of where we have seen attacks, and attacks come from many different places, and there are attacks on many different cybersecurity systems. So I want to thank Mr. NYE for this amendment, and I urge my colleagues to support it.

I reserve the balance of my time.

Mr. MCCAUL. Mr. Chairman, I rise to claim time in opposition to this amendment, although I am not opposed to it.

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

There was no objection.

Mr. MCCAUL. Mr. Chairman, this amendment would simply ask the General Accounting Office to examine the current cybersecurity infrastructure and report to Congress with recommendations on how to address any failings or weaknesses within the infrastructure and the technology available to do so. Therefore, I support this amendment, and I also urge my colleagues to do so.

I yield back the balance of my time.

Mr. LIPINSKI. Mr. Chairman, I yield such time as he may consume to the gentleman from Virginia (Mr. NYE).

Mr. NYE. I would like to thank my colleague for yielding. Mr. Chair, first I would like to thank Chairman GORDON and Ranking Member HALL for their important work on this bill, to improve our cybersecurity and strengthen the partnerships between the Federal Government and the private sector.

Cybersecurity is an issue of national security, and as we work to defend against the next generation of cyberthreats, the only way to make sure we're getting it right is to find out what we're doing wrong. That's why I have introduced an amendment to require the GAO to conduct a study, examining key weaknesses within the current cybersecurity infrastructure along with recommendations on how to address such weaknesses in the future and on the technology that is needed to do so.

Not only will this benefit Federal and private sector efforts to strengthen cybersecurity, but it will also help local cities and counties learn how to defend themselves against attacks on their networks and infrastructure.

In my district in Virginia, in the city of Hampton, we are doing exactly that. We are creating a regional Center of Excellence to help local communities improve their cybersecurity. This bill will help that effort, and the GAO report called for in my amendment will make it even stronger.

I would like to thank my colleagues for their support. I urge the rest of my colleagues to join me in supporting this amendment and in passing this bill.

Mr. LIPINSKI. I yield back the balance of my time.

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

The amendment was agreed to.

AMENDMENT NO. 24 OFFERED BY MR. OWENS

The Acting CHAIR. It is now in order to consider amendment No. 24 printed in House Report 111–410.

Mr. OWENS. I have an amendment at the desk.

The Acting CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Amendment No. 24 offered by Mr. OWENS:

Page 6, line 24, insert '', including technologies to secure sensitive information shared among Federal agencies'' after ''digital infrastructure''.

The Acting CHAIR. Pursuant to House Resolution 1051, the gentleman from New York (Mr. OWENS) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentleman from New York.

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

I would first like to thank Chairman GORDON and the committee for their work on this important bipartisan legislation. My amendment would expand the cybersecurity strategic R&D plan, created under H.R. 4061, by adding a component to address information sharing between Federal agencies.

Information technology has advanced rapidly in the last two decades, benefiting nearly every sector of our economy; but our dependence on IT in many ways increased our exposure to unconventional attacks. H.R. 4061 will help address our vulnerabilities by creating an overall vision for the Federal cybersecurity R&D portfolio. Improving the coordination of cybersecurity research and development activities is the first step in preventing a catastrophic attack on our IT infrastructure. Mr. Chairman, my amendment would improve the strategic R&D plan by including a component on technologies to secure sensitive information shared among Federal agencies.

Our Nation's security is at risk without protections in place to safeguard the flow of information within the Federal Government. I believe the amendment I am offering today gets at the heart of addressing this problem, and I urge its adoption.

With that, I reserve the balance of my time.

Mr. MCCAUL. Mr. Chairman, I rise to claim time in opposition to this amendment, although I am not opposed to it.

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

There was no objection.

Mr. MCCAUL. Mr. Chairman, this amendment simply states that ''technologies to secure sensitive information among Federal agencies'' shall be among the technologies addressed in the interagency cybersecurity R&D plan required by the bill. As I understand it, the gentleman's amendment is referring to information controlled by the Federal Government that is not classified but is still sensitive and particularly important to protect. This class of information is very substantial in numerous Federal agencies, including our research and development agencies, and I believe it's reasonable and appropriate to consider how best to pursue technologies that may assist in better protecting it without classifying the information outright. So therefore, I support the gentleman's amendment. I urge my colleagues to do so.

I yield back the balance of my time.

Mr. OWENS. In closing, I want to again thank the chairman, the ranking member, and the committee for their work. I urge support for my amendment and for the underlying bill.

I yield back the balance of my time.

The Acting CHAIR. The question is on the amendment offered by the gentleman from New York (Mr. OWENS).

The question was taken; and the Acting Chair announced that the ayes appeared to have it.

Mr. OWENS. Mr. Chairman, I demand a recorded vote.

The Acting CHAIR. Pursuant to clause 6 of rule XVIII, further proceedings on the amendment offered by the gentleman from New York will be postponed.

AMENDMENT NO. 25 OFFERED BY MR. HEINRICH

The Acting CHAIR. It is now in order to consider amendment No. 25 printed in House Report 111–410.

Mr. HEINRICH. Mr. Chair, I have an amendment at the desk.

The Acting CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Amendment No. 25 offered by Mr. HEINRICH:

Page 8, line 20, insert ''National Laboratories,'' after ''minority serving institutions,''.

The Acting CHAIR. Pursuant to House Resolution 1051, the gentleman from New Mexico (Mr. HEINRICH) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentleman from New Mexico.

Mr. HEINRICH. Mr. Chair, this legislation is critical to our national security, and I want to thank Representative DAN LIPINSKI and Chairman BART GORDON for their leadership. We have made some incredible advancements in the use of technology in the 21st century; and with much of our Nation's public and private commerce taking place on the Internet, defending our cyberspace from cybercriminals and cyberterrorism has never been more vital to our national security.

In central New Mexico, Sandia National Laboratories dedicated roughly $20 million last year to this very cause. Sandia has also created a program to train our future workforce by working directly alongside Sandia researchers to secure systems and examine attack modes. Sandia National Labs is a leader in defensive cybersecurity research and development for our Nation's intelligence community and has been home to countless high-level security advancements.

For decades, national laboratories across the Nation have worked to protect their own data and networks from intrusion. Of necessity, they have developed expertise in cryptography as well as sophisticated techniques to detect and thwart cyberattacks. This amendment simply includes our national labs as contributing stakeholders to the strategic management plan for cybersecurity research. Including our national labs and utilizing their cybersecurity expertise is critical to keeping our Nation's cyberspace secure, and I would urge my colleagues to support this amendment.

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

Mr. MCCAUL. Mr. Chairman, I rise to claim time in opposition to this amendment, although I am not opposed to it.

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

There was no objection.

Mr. MCCAUL. Let me say, Mr. Chairman, I believe this is our last amendment, and I want to commend the chairman for his perseverance through 25 amendments here today.

This amendment simply adds national laboratories to the list of stakeholders that the administration should engage in developing its strategic plan for R&D. I think it's a good idea. I urge support. I urge my colleagues to support it.

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

Mr. HEINRICH. I simply urge my colleagues' support and yield to the gentleman from Illinois (Mr. LIPINSKI).

Mr. LIPINSKI. I would like to thank Mr. HEINRICH for working with the committee on amendment language. I have visited Sandia. We also have great work going on in my own backyard at Argonne National Lab on cybersecurity. There is a lot of great work going on at all of our labs and contributing so much behind the scenes to things that we don't see. So I want to thank Mr. HEINRICH for his amendment. I urge my colleagues to support it.

But in closing, on their last amendment here, I also would like to thank Mr. MCCAUL for all of his work. This is the way the American people want to see us work, work together, Democrats and Republicans. We work very well together on the Science and Technology Committee. It's an important issue that impacts people in their everyday lives. The amount of time that all of us spend on the Internet, the vulnerabilities that are out there, hopefully through this work, I know that we can really make things better, make the Internet more secure so we have fewer problems with attacks not just on the government but on individuals.

Again, I would like to thank Mr. MCCAUL, Chairman GORDON, and everyone who has worked together on this.

Mr. MCCAUL. Will the gentleman yield?

Mr. LIPINSKI. I yield to the gentleman from Texas.

Mr. MCCAUL. Thank you. Mr. Chairman, I just wanted to personally commend the gentleman for the authorship of this bill. I was proud to be a lead sponsor of the bill. When it comes to security matters and, I think, a lot of science and technology matters, we work in a very bipartisan way. Again, I think that's what the American people really want and deserve out of this Congress. So I am glad that we saw a little bit of that bipartisanship here today on the House floor. And thank you for your leadership.

Mr. LIPINSKI. I thank the gentleman from Texas (Mr. MCCAUL), and I urge my colleagues to support this amendment and to support the bill.

I yield back the balance of my time.

The Acting CHAIR. The question is on the amendment offered by the gentleman from New Mexico (Mr. HEINRICH).

The amendment was agreed to.

□ 1545

ANNOUNCEMENT BY THE ACTING CHAIR

The Acting CHAIR. Pursuant to clause 6 of rule XVIII, proceedings will now resume on those amendments printed in House Report 111–410 on which further proceedings were postponed, in the following order:

Amendment No. 1 by Mr. HASTINGS of Florida;

Amendment No. 3 by Mr. FLAKE of Arizona;

Amendment No. 8 by Mrs. DAHLKEMPER of Pennsylvania;

Amendment No. 14 by Mr. CUELLAR of Texas;

Amendment No. 18 by Mr. CONNOLLY of Virginia.

The Chair will reduce to 5 minutes the time for any electronic vote after the first vote in this series.

AMENDMENT NO. 1 OFFERED BY MR. HASTINGS OF FLORIDA

The Acting CHAIR. The unfinished business is the demand for a recorded vote on the amendment offered by the gentleman from Florida (Mr. HASTINGS) on which further proceedings were postponed and on which the ayes prevailed by voice vote.

The Clerk will redesignate the amendment.

The Clerk redesignated the amendment.

RECORDED VOTE

The Acting CHAIR. A recorded vote has been demanded.

A recorded vote was ordered.

The vote was taken by electronic device, and there were—ayes 417, noes 5, not voting 17, as follows:

[Roll No. 34]

AYES—417

Abercrombie	Castle	Frelinghuysen
Ackerman	Castor (FL)	Fudge
Aderholt	Chaffetz	Gallegly
Adler (NJ)	Chandler	Garamendi
Akin	Childers	Garrett (NJ)
Alexander	Chu	Gerlach
Altmire	Clarke	Giffords
Andrews	Clay	Gingrey (GA)
Arcuri	Cleaver	Gonzalez
Austria	Clyburn	Goodlatte
Baca	Coble	Gordon (TN)
Bachmann	Coffman (CO)	Granger
Bachus	Cohen	Graves
Baird	Cole	Grayson
Baldwin	Conaway	Green, Al
Barrow	Connolly (VA)	Green, Gene
Bartlett	Conyers	Griffith
Barton (TX)	Cooper	Grijalva
Bean	Costa	Guthrie
Becerra	Costello	Hall (NY)
Berkley	Courtney	Hall (TX)
Berman	Crenshaw	Halvorson
Berry	Crowley	Hare
Biggert	Cuellar	Harman
Bilbray	Culberson	Harper
Bilirakis	Cummings	Hastings (FL)
Bishop (GA)	Dahlkemper	Hastings (WA)
Bishop (NY)	Davis (AL)	Heinrich
Bishop (UT)	Davis (CA)	Heller
Blackburn	Davis (IL)	Hensarling
Blumenauer	Davis (KY)	Herger
Blunt	Davis (TN)	Herseth Sandlin
Boccieri	Deal (GA)	Higgins
Boehner	DeFazio	Hill
Bonner	DeGette	Himes
Bono Mack	Delahunt	Hinchey
Boozman	DeLauro	Hinojosa
Bordallo	Dent	Hirono
Boren	Diaz-Balart, L.	Hodes
Boswell	Diaz-Balart, M.	Hoekstra
Boucher	Dicks	Holden
Boustany	Dingell	Holt
Boyd	Doggett	Honda
Brady (PA)	Donnelly (IN)	Hoyer
Brady (TX)	Doyle	Hunter
Braley (IA)	Dreier	Inglis
Bright	Driehaus	Inslee
Brown (SC)	Duncan	Israel
Brown, Corrine	Edwards (MD)	Issa
Brown-Waite, Ginny	Edwards (TX)	Jackson (IL)
Buchanan	Ehlers	Jackson Lee (TX)
Burgess	Ellison	Jenkins
Burton (IN)	Ellsworth	Johnson (GA)
Butterfield	Emerson	Johnson (IL)
Buyer	Engel	Johnson, Sam
Calvert	Eshoo	Jones
Camp	Etheridge	Jordan (OH)
Campbell	Faleomavaega	Kagen
Cantor	Fallin	Kanjorski
Cao	Farr	Kaptur
Capito	Fattah	Kennedy
Capps	Filner	Kildee
Capuano	Flake	Kilpatrick (MI)
Cardoza	Fleming	Kilroy
Carnahan	Forbes	Kind
Carney	Fortenberry	King (IA)
Carson (IN)	Foster	King (NY)
Carter	Foxx	Kingston
Cassidy	Frank (MA)	Kissell
	Franks (AZ)	

Klein (FL)
Kline (MN)
Kosmas
Kratovil
Kucinich
Lamborn
Lance
Langevin
Larsen (WA)
Larson (CT)
Latham
LaTourette
Latta
Lee (CA)
Lee (NY)
Levin
Lewis (CA)
Lewis (GA)
Linder
Lipinski
LoBiondo
Loebsack
Lofgren, Zoe
Lowey
Lucas
Luetkemeyer
Luján
Lummis
Lungren, Daniel E.
Lynch
Maffei
Maloney
Manzullo
Marchant
Markey (CO)
Markey (MA)
Marshall
Matheson
Matsui
McCarthy (CA)
McCarthy (NY)
McCaul
McCollum
McCotter
McDermott
McGovern
McHenry
McIntyre
McKeon
McMahon
McMorris Rodgers
McNerney
Meek (FL)
Meeks (NY)
Melancon
Mica
Michaud
Miller (FL)
Miller (MI)
Miller (NC)
Miller, Gary
Miller, George
Minnick
Mitchell
Mollohan
Moore (KS)
Moore (WI)
Moran (KS)
Moran (VA)
Murphy (CT)
Murphy (NY)
Murphy, Patrick
Murphy, Tim
Myrick
Napolitano
Neal (MA)
Neugebauer
Norton
Nunes
Nye
Oberstar
Obey
Olson
Olver
Ortiz
Owens
Pallone
Pascrell
Pastor (AZ)
Paulsen
Payne
Pence
Perlmutter
Perriello
Peters
Peterson
Petri
Pierluisi
Pingree (ME)
Pitts
Platts
Polis (CO)
Pomeroy
Posey
Price (GA)
Price (NC)
Putnam
Quigley
Rahall
Rangel
Rehberg
Reichert
Reyes
Richardson
Rodriguez
Roe (TN)
Rogers (AL)
Rogers (KY)
Rogers (MI)
Rohrabacher
Rooney
Ros-Lehtinen
Roskam
Ross
Rothman (NJ)
Roybal-Allard
Royce
Ruppersberger
Ryan (WI)
Sablan
Salazar
Sanchez, Loretta
Sarbanes
Scalise
Schakowsky
Schauer
Schiff
Schmidt
Schock
Schrader
Schwartz
Scott (GA)
Scott (VA)
Sensenbrenner
Serrano
Sessions
Sestak
Shadegg
Shea-Porter
Sherman
Shimkus
Shuler
Shuster
Simpson
Sires
Skelton
Slaughter
Smith (NE)
Smith (NJ)
Smith (TX)
Smith (WA)
Snyder
Souder
Space
Speier
Spratt
Stark
Stearns
Stupak
Sullivan
Sutton
Tanner
Taylor
Teague
Terry
Thompson (CA)
Thompson (MS)
Thompson (PA)
Thornberry
Tiahrt
Tiberi
Tierney
Titus
Towns
Tsongas
Turner
Upton
Van Hollen
Velázquez
Visclosky
Walden
Walz
Wamp
Wasserman Schultz
Waters
Watson
Watt
Waxman
Weiner
Welch
Westmoreland
Whitfield
Wilson (OH)
Wilson (SC)
Wittman
Wolf
Wu
Yarmuth
Young (AK)

NOES—5

Broun (GA)
Mack
McClintock
Paul
Poe (TX)

NOT VOTING—17

Barrett (SC)
Christensen
Gohmert
Gutierrez
Johnson, E. B.
Kirk
Kirkpatrick (AZ)
Massa
Murtha
Nadler (NY)
Radanovich
Rush
Ryan (OH)
Sánchez, Linda T.
Tonko
Woolsey
Young (FL)

□ 1611

Mr. PAUL of Texas changed his vote from ''aye'' to ''no.''

Mrs. MALONEY and Mr. GARY G. MILLER of California changed their vote from ''no'' to ''aye.''

So the amendment was agreed to.

The result of the vote was announced as above recorded.

Stated for:

Mr. TONKO. Mr. Chair, on rollcall No. 34 I was unavoidably detained. Had I been present, I would have voted "aye."

AMENDMENT NO. 3 OFFERED BY MR. FLAKE

The Acting CHAIR (Mr. PIERLUISI). The unfinished business is the demand for a recorded vote on the amendment offered by the gentleman from Arizona (Mr. FLAKE) on which further proceedings were postponed and on which the ayes prevailed by voice vote.

The Clerk will redesignate the amendment.

The Clerk redesignated the amendment.

RECORDED VOTE

The Acting CHAIR. A recorded vote has been demanded.

A recorded vote was ordered.

The Acting CHAIR. This is a 5-minute vote.

The vote was taken by electronic device, and there were—ayes 396, noes 31, not voting 12, as follows:

[Roll No. 35]

AYES—396

Abercrombie
Ackerman
Aderholt
Adler (NJ)
Akin
Alexander
Altmire
Andrews
Arcuri
Austria
Baca
Bachmann
Bachus
Baird
Baldwin
Barrow
Bartlett
Barton (TX)
Bean
Becerra
Berkley
Biggert
Bilbray
Bilirakis
Bishop (GA)
Bishop (NY)
Bishop (UT)
Blackburn
Blumenauer
Blunt
Boccieri
Boehner
Bonner
Bono Mack
Boozman
Bordallo
Boren
Boswell
Boucher
Boustany
Boyd
Brady (PA)
Brady (TX)
Braley (IA)
Bright
Broun (GA)
Brown (SC)
Brown-Waite, Ginny
Buchanan
Burgess
Burton (IN)
Butterfield
Buyer
Calvert
Camp
Campbell
Cantor
Cao
Capito
Capps
Capuano
Cardoza
Carnahan
Carney
Carson (IN)
Carter
Cassidy
Castle
Castor (FL)
Chaffetz
Chandler
Childers
Chu
Clay
Cleaver
Coble
Coffman (CO)
Cohen
Cole
Conaway
Connolly (VA)
Cooper
Costa
Costello
Courtney
Crenshaw
Cuellar
Culberson
Cummings
Dahlkemper
Davis (AL)
Davis (CA)
Davis (IL)
Davis (KY)
Davis (TN)
Deal (GA)
DeFazio
DeGette
Delahunt
DeLauro
Dent
Diaz-Balart, L.
Diaz-Balart, M.
Dicks
Dingell
Doggett
Donnelly (IN)
Doyle
Dreier
Driehaus
Duncan
Edwards (TX)
Ehlers
Ellison
Ellsworth
Emerson
Engel
Eshoo
Etheridge
Faleomavaega
Fallin
Farr
Fattah
Flake
Fleming
Forbes
Fortenberry
Foster
Foxx
Frank (MA)
Franks (AZ)
Frelinghuysen
Gallegly
Garamendi
Garrett (NJ)
Gerlach
Giffords
Gingrey (GA)
Gohmert
Gonzalez
Goodlatte
Gordon (TN)
Granger
Graves
Grayson
Green, Al
Green, Gene
Griffith
Guthrie
Hall (TX)
Halvorson
Hare
Harman
Harper
Hastings (WA)
Heinrich
Heller
Hensarling
Herger
Herseth Sandlin
Higgins
Hill
Himes
Hinchey
Hinojosa
Hirono
Hodes
Hoekstra
Holden
Holt
Honda
Hoyer
Hunter
Inglis
Inslee
Israel
Issa
Jackson (IL)
Jackson Lee (TX)
Jenkins
Johnson (GA)
Johnson (IL)
Johnson, Sam
Jordan (OH)
Kagen
Kanjorski
Kaptur
Kildee
Kilpatrick (MI)
Kilroy
Kind
King (IA)
King (NY)
Kingston
Kissell
Klein (FL)
Kline (MN)
Kosmas
Kratovil
Lamborn
Lance
Langevin
Larsen (WA)
Larson (CT)
Latham
LaTourette
Latta
Lee (NY)
Levin
Lewis (CA)
Lewis (GA)
Linder
Lipinski
LoBiondo
Loebsack
Lofgren, Zoe
Lowey
Lucas
Luetkemeyer
Luján
Lummis
Lungren, Daniel E.
Lynch
Mack
Maffei
Maloney
Manzullo
Marchant
Markey (CO)
Markey (MA)
Marshall
Matheson
Matsui
McCarthy (CA)
McCarthy (NY)
McCaul
McClintock
McCollum
McCotter
McDermott
McGovern
McHenry
McIntyre
McKeon
McMahon
McMorris Rodgers
McNerney
Meek (FL)
Meeks (NY)
Melancon
Mica
Michaud
Miller (FL)
Miller (MI)
Miller (NC)
Miller, Gary
Miller, George
Minnick
Mitchell
Mollohan
Moore (KS)
Moran (KS)
Moran (VA)
Murphy (CT)
Murphy (NY)
Murphy, Patrick
Murphy, Tim
Myrick
Napolitano
Neal (MA)
Neugebauer
Norton
Nunes
Nye
Oberstar
Obey
Olson
Olver
Ortiz
Owens
Pallone
Pascrell
Pastor (AZ)
Paulsen
Pence
Perlmutter
Perriello
Peters
Peterson
Petri
Pierluisi
Pingree (ME)
Pitts
Platts
Poe (TX)
Polis (CO)
Pomeroy
Posey
Price (GA)
Price (NC)
Putnam
Quigley
Rangel
Rehberg
Reichert
Reyes
Richardson
Rodriguez
Roe (TN)
Rogers (AL)
Rogers (KY)
Rogers (MI)
Rohrabacher
Rooney
Ros-Lehtinen
Roskam
Ross
Roybal-Allard
Royce
Ryan (WI)
Sablan
Salazar
Sanchez, Loretta
Sarbanes
Scalise
Schakowsky
Schauer
Schiff
Schmidt
Schock
Schrader
Schwartz
Scott (GA)
Scott (VA)
Sensenbrenner
Serrano
Sessions
Sestak
Shadegg
Shea-Porter
Shimkus
Shuler
Shuster
Simpson
Sires
Skelton
Slaughter
Smith (NE)
Smith (NJ)
Smith (TX)
Smith (WA)
Snyder
Souder
Space
Speier
Spratt
Stark
Stearns
Stupak
Sullivan
Sutton
Tanner
Taylor
Teague
Terry
Thompson (CA)
Thompson (MS)
Thompson (PA)
Thornberry
Tiahrt
Tiberi
Tierney
Titus
Tonko
Towns
Tsongas
Turner
Upton
Van Hollen
Velázquez
Visclosky
Walden
Walz
Wamp
Wasserman Schultz
Waxman
Weiner
Welch
Westmoreland
Whitfield
Wilson (OH)
Wilson (SC)
Wittman
Wolf
Wu
Yarmuth

NOES—31

Berman
Berry
Brown, Corrine
Clarke
Clyburn
Conyers
Crowley
Edwards (MD)
Filner
Fudge
Grijalva
Hall (NY)
Hastings (FL)
Jones
Kennedy
Kucinich
Lee (CA)
Moore (WI)
Nadler (NY)
Paul
Payne
Rahall
Rothman (NJ)
Ruppersberger
Ryan (OH)
Sherman
Waters
Watson
Watt
Woolsey
Young (AK)

NOT VOTING—12

Barrett (SC)
Christensen
Gutierrez
Johnson, E. B.
Kirk
Kirkpatrick (AZ)
Massa
Murtha
Radanovich
Rush
Sánchez, Linda T.
Young (FL)

ANNOUNCEMENT BY THE ACTING CHAIR

The Acting CHAIR (during the vote). Members are reminded that there are 2 minutes remaining in this vote.

□ 1622

Messrs. SHERMAN, KUCINICH, KENNEDY, BERRY, HASTINGS of Florida,

CONYERS, Ms. EDWARDS of Maryland, and Ms. WATERS changed their vote from ''aye'' to ''no.''

Ms. JACKSON LEE of Texas, Ms. BORDALLO and Mr. AL GREEN of Texas changed their vote from ''no'' to ''aye.''

So the amendment was agreed to.

The result of the vote was announced as above recorded.

AMENDMENT NO. 8 OFFERED BY MRS. DAHLKEMPER

The Acting CHAIR. The unfinished business is the demand for a recorded vote on the amendment offered by the gentlewoman from Pennsylvania (Mrs. DAHLKEMPER) on which further proceedings were postponed and on which the ayes prevailed by voice vote.

The Clerk will redesignate the amendment.

The Clerk redesignated the amendment.

RECORDED VOTE

The Acting CHAIR. A recorded vote has been demanded.

A recorded vote was ordered.

The Acting CHAIR. This will be a 5-minute vote.

The vote was taken by electronic device, and there were—ayes 419, noes 3, not voting 17, as follows:

[Roll No. 36]

AYES—419

Abercrombie
Ackerman
Aderholt
Adler (NJ)
Akin
Alexander
Altmire
Andrews
Arcuri
Austria
Baca
Bachmann
Bachus
Baird
Baldwin
Barrow
Bartlett
Barton (TX)
Bean
Becerra
Berkley
Berman
Berry
Biggert
Bilbray
Bilirakis
Bishop (GA)
Bishop (NY)
Bishop (UT)
Blackburn
Blumenauer
Blunt
Boccieri
Bonner
Bono Mack
Boozman
Bordallo
Boren
Boswell
Boucher
Boustany
Boyd
Brady (PA)
Brady (TX)
Braley (IA)
Bright
Broun (GA)
Brown (SC)
Brown, Corrine
Brown-Waite, Ginny
Buchanan
Burgess
Burton (IN)
Butterfield
Buyer
Calvert
Camp
Campbell
Cantor
Cao
Capito
Capps
Capuano
Cardoza
Carnahan
Carney
Carson (IN)
Carter
Cassidy
Castle
Castor (FL)
Chaffetz
Chandler
Childers
Chu
Clarke
Clay
Cleaver
Clyburn
Coble
Coffman (CO)
Cohen
Cole
Conaway
Connolly (VA)
Conyers
Cooper
Costa
Costello
Courtney
Crenshaw
Crowley
Cuellar
Culberson
Cummings
Dahlkemper
Davis (AL)
Davis (CA)
Davis (IL)
Davis (KY)
Davis (TN)
Deal (GA)
DeFazio
DeGette
Delahunt
DeLauro
Dent
Diaz-Balart, L.
Diaz-Balart, M.
Dicks
Dingell
Doggett
Donnelly (IN)
Doyle
Dreier
Driehaus
Duncan
Edwards (MD)
Edwards (TX)
Ehlers
Ellison
Ellsworth
Emerson
Engel
Eshoo
Etheridge
Faleomavaega
Fallin
Farr
Fattah
Filner
Fleming
Forbes
Fortenberry
Foxx
Frank (MA)
Franks (AZ)
Frelinghuysen
Fudge
Gallegly
Garrett (NJ)
Gerlach
Giffords
Gingrey (GA)
Gohmert
Gonzalez
Goodlatte
Gordon (TN)
Granger
Graves
Grayson
Green, Al
Green, Gene
Griffith
Grijalva
Guthrie
Hall (NY)
Hall (TX)
Halvorson
Hare
Harman
Harper
Hastings (FL)
Hastings (WA)
Heinrich
Heller
Hensarling
Herger
Herseth Sandlin
Higgins
Hill
Himes
Hinchey
Hinojosa
Hirono
Hodes
Hoekstra
Holden
Holt
Honda
Hoyer
Hunter
Inglis
Inslee
Israel
Issa
Jackson (IL)
Jackson Lee (TX)
Jenkins
Johnson (GA)
Johnson (IL)
Johnson, Sam
Jones
Jordan (OH)
Kagen
Kanjorski
Kaptur
Kennedy
Kildee
Kilpatrick (MI)
Kilroy
Kind
King (IA)
King (NY)
Kingston
Kissell
Klein (FL)
Kline (MN)
Kosmas
Kratovil
Kucinich
Lamborn
Lance
Langevin
Larsen (WA)
Larson (CT)
Latham
LaTourette
Latta
Lee (CA)
Lee (NY)
Levin
Lewis (CA)
Lewis (GA)
Linder
Lipinski
LoBiondo
Loebsack
Lofgren, Zoe
Lowey
Lucas
Luetkemeyer
Luján
Lummis
Lungren, Daniel E.
Lynch
Mack
Maffei
Maloney
Manzullo
Marchant
Markey (CO)
Markey (MA)
Marshall
Matheson
Matsui
McCarthy (CA)
McCarthy (NY)
McCaul
McCollum
McCotter
McDermott
McGovern
McHenry
McIntyre
McKeon
McMahon
McMorris Rodgers
McNerney
Meek (FL)
Meeks (NY)
Melancon
Mica
Michaud
Miller (FL)
Miller (MI)
Miller (NC)
Miller, Gary
Miller, George
Minnick
Mitchell
Mollohan
Moore (KS)
Moore (WI)
Moran (KS)
Moran (VA)
Murphy (NY)
Murphy, Patrick
Murphy, Tim
Myrick
Nadler (NY)
Napolitano
Neal (MA)
Neugebauer
Norton
Nunes
Nye
Oberstar
Obey
Olson
Olver
Ortiz
Owens
Pallone
Pascrell
Pastor (AZ)
Paulsen
Payne
Pence
Perlmutter
Perriello
Peters
Peterson
Petri
Pierluisi
Pingree (ME)
Pitts
Platts
Poe (TX)
Polis (CO)
Pomeroy
Posey
Price (GA)
Price (NC)
Putnam
Quigley
Rahall
Rangel
Rehberg
Reichert
Reyes
Richardson
Rodriguez
Roe (TN)
Rogers (AL)
Rogers (KY)
Rogers (MI)
Rohrabacher
Rooney
Ros-Lehtinen
Roskam
Ross
Rothman (NJ)
Roybal-Allard
Royce
Ruppersberger
Ryan (OH)
Ryan (WI)
Sablan
Salazar
Sanchez, Loretta
Sarbanes
Scalise
Schakowsky
Schauer
Schiff
Schmidt
Schock
Schrader
Schwartz
Scott (GA)
Scott (VA)
Sensenbrenner
Serrano
Sessions
Sestak
Shadegg
Shea-Porter
Sherman
Shimkus
Shuler
Shuster
Simpson
Sires
Skelton
Smith (NE)
Smith (NJ)
Smith (TX)
Smith (WA)
Snyder
Souder
Space
Speier
Spratt
Stark
Stearns
Stupak
Sullivan
Sutton
Tanner
Taylor
Teague
Terry
Thompson (CA)
Thompson (MS)
Thompson (PA)
Thornberry
Tiahrt
Tiberi
Tierney
Titus
Tonko
Towns
Tsongas
Turner
Upton
Van Hollen
Velázquez
Visclosky
Walden
Walz
Wamp
Wasserman Schultz
Waters
Watson
Watt
Waxman
Weiner
Welch
Westmoreland
Whitfield
Wilson (OH)
Wilson (SC)
Wittman
Wolf
Woolsey
Wu
Yarmuth
Young (AK)

NOES—3

Flake
McClintock
Paul

NOT VOTING—17

Barrett (SC)
Boehner
Christensen
Foster
Garamendi
Gutierrez
Johnson, E. B.
Kirk
Kirkpatrick (AZ)
Massa
Murphy (CT)
Murtha
Radanovich
Rush
Sánchez, Linda T.
Slaughter
Young (FL)

□ 1630

Messrs. FLAKE and PAUL changed their vote from ''aye'' to ''no.''

So the amendment was agreed to.

The result of the vote was announced as above recorded.

AMENDMENT NO. 14 OFFERED BY MR. CUELLAR

The Acting CHAIR. The unfinished business is the demand for a recorded vote on the amendment offered by the gentleman from Texas (Mr. CUELLAR) on which further proceedings were postponed and on which the ayes prevailed by voice vote.

The Clerk will redesignate the amendment.

The Clerk redesignated the amendment.

RECORDED VOTE

The Acting CHAIR. A recorded vote has been demanded.

A recorded vote was ordered.

The Acting CHAIR. This will be a 5-minute vote.

The vote was taken by electronic device, and there were—ayes 416, noes 4, not voting 19, as follows:

[Roll No. 37]

AYES—416

Abercrombie
Ackerman
Aderholt
Adler (NJ)
Akin
Alexander
Altmire
Andrews
Arcuri
Austria
Baca
Bachmann
Bachus
Baird
Baldwin
Barrow
Bartlett
Barton (TX)
Bean
Becerra
Berkley
Berman
Berry
Biggert
Bilbray
Bilirakis
Bishop (GA)
Bishop (NY)
Bishop (UT)
Blackburn
Blumenauer
Blunt
Boccieri
Boehner
Bonner
Bono Mack
Boozman
Bordallo
Boren
Boswell
Boucher
Boustany
Boyd
Brady (PA)
Brady (TX)
Braley (IA)
Bright
Brown (SC)
Brown, Corrine
Brown-Waite, Ginny
Buchanan
Burgess
Burton (IN)
Butterfield
Buyer
Calvert
Camp
Campbell
Cantor
Cao
Capito
Capps
Capuano
Cardoza
Carnahan
Carney
Carson (IN)
Carter
Cassidy
Castle
Castor (FL)
Chaffetz
Chandler
Childers
Chu
Clarke
Clay
Cleaver
Clyburn
Coble
Coffman (CO)
Cohen
Cole
Conaway
Connolly (VA)
Conyers
Cooper
Costa
Costello
Courtney
Crenshaw
Crowley
Cuellar
Culberson
Cummings
Dahlkemper
Davis (AL)
Davis (CA)
Davis (IL)
Davis (KY)
Davis (TN)
Deal (GA)
DeFazio
DeGette
Delahunt
DeLauro
Dent
Diaz-Balart, L.
Diaz-Balart, M.
Dicks
Dingell
Doggett
Donnelly (IN)
Doyle
Dreier
Driehaus
Duncan
Edwards (MD)
Edwards (TX)
Ehlers
Ellison
Ellsworth
Emerson
Engel
Eshoo
Etheridge
Faleomavaega
Fallin
Farr
Fattah
Filner
Fleming
Forbes
Fortenberry
Foster
Foxx
Frank (MA)
Franks (AZ)
Frelinghuysen
Fudge
Gallegly
Garamendi
Garrett (NJ)
Gerlach
Giffords
Gohmert
Gonzalez
Goodlatte
Gordon (TN)
Granger
Graves
Grayson
Green, Al
Green, Gene
Griffith
Grijalva
Guthrie
Hall (NY)
Hall (TX)
Halvorson
Hare
Harman
Harper
Hastings (FL)
Hastings (WA)
Heinrich
Heller
Hensarling
Herger
Herseth Sandlin
Higgins
Hill
Himes
Hinchey
Hinojosa
Hirono
Hodes
Hoekstra
Holden

Holt
Honda
Hoyer
Hunter
Inglis
Inslee
Israel
Issa
Jackson (IL)
Jackson Lee (TX)
Jenkins
Johnson (GA)
Johnson (IL)
Johnson, Sam
Jones
Jordan (OH)
Kagen
Kanjorski
Kaptur
Kennedy
Kildee
Kilpatrick (MI)
Kilroy
Kind
King (IA)
King (NY)
Kingston
Kissell
Klein (FL)
Kline (MN)
Kosmas
Kratovil
Kucinich
Lamborn
Lance
Langevin
Larsen (WA)
Larson (CT)
Latham
LaTourette
Latta
Lee (CA)
Lee (NY)
Levin
Lewis (CA)
Linder
Lipinski
LoBiondo
Loebsack
Lofgren, Zoe
Lowey
Lucas
Luetkemeyer
Luján
Lummis
Lungren, Daniel E.
Lynch
Mack
Maffei
Maloney
Manzullo
Marchant
Markey (CO)
Markey (MA)
Marshall
Matheson
Matsui
McCarthy (CA)
McCarthy (NY)
McCaul
McCollum
McCotter
McDermott
McGovern
McHenry
McIntyre
McKeon
McMahon
McMorris Rodgers
McNerney
Meek (FL)
Meeks (NY)
Melancon
Mica
Michaud
Miller (FL)
Miller (MI)
Miller (NC)
Miller, Gary
Miller, George
Minnick
Mitchell
Mollohan
Moore (KS)
Moore (WI)
Moran (KS)
Moran (VA)
Murphy (CT)
Murphy (NY)
Murphy, Patrick
Murphy, Tim
Myrick
Nadler (NY)
Neal (MA)
Neugebauer
Nunes
Nye
Oberstar
Obey
Olson
Olver
Ortiz
Owens
Pallone
Pascrell
Pastor (AZ)
Paulsen
Payne
Pence
Perlmutter
Perriello
Peters
Peterson
Petri
Pierluisi
Pingree (ME)
Pitts
Platts
Poe (TX)
Polis (CO)
Pomeroy
Posey
Price (GA)
Price (NC)
Putnam
Quigley
Rahall
Rehberg
Reichert
Reyes
Richardson
Rodriguez
Roe (TN)
Rogers (AL)
Rogers (KY)
Rogers (MI)
Rohrabacher
Rooney
Ros-Lehtinen
Roskam
Ross
Rothman (NJ)
Roybal-Allard
Royce
Ruppersberger
Ryan (OH)
Ryan (WI)
Sablan
Salazar
Sanchez, Loretta
Sarbanes
Scalise
Schakowsky
Schauer
Schiff
Schmidt
Schock
Schrader
Schwartz
Scott (GA)
Scott (VA)
Sensenbrenner
Serrano
Sessions
Sestak
Shadegg
Shea-Porter
Sherman
Shimkus
Shuler
Shuster
Simpson
Sires
Skelton
Smith (NE)
Smith (NJ)
Smith (TX)
Smith (WA)
Snyder
Souder
Space
Speier
Spratt
Stark
Stearns
Stupak
Sullivan
Sutton
Tanner
Taylor
Teague
Terry
Thompson (CA)
Thompson (MS)
Thompson (PA)
Thornberry
Tiahrt
Tiberi
Tierney
Titus
Tonko
Towns
Turner
Upton
Van Hollen
Velázquez
Visclosky
Walden
Walz
Wamp
Wasserman Schultz
Waters
Watson
Watt
Waxman
Weiner
Welch
Westmoreland
Whitfield
Wilson (OH)
Wilson (SC)
Wittman
Wolf
Woolsey
Wu
Yarmuth
Young (AK)

NOES—4

Broun (GA)
Flake
McClintock
Paul

NOT VOTING—19

Barrett (SC)
Christensen
Gingrey (GA)
Gutierrez
Johnson, E. B.
Kirk
Kirkpatrick (AZ)
Lewis (GA)
Massa
Murtha
Napolitano
Norton
Radanovich
Rangel
Rush
Sánchez, Linda T.
Slaughter
Tsongas
Young (FL)

ANNOUNCEMENT BY THE ACTING CHAIR

The Acting CHAIR (during the vote). Members are advised that 2 minutes remain on this vote.

□ 1638

So the amendment was agreed to.

The result of the vote was announced as above recorded.

AMENDMENT NO. 18 OFFERED BY MR. CONNOLLY OF VIRGINIA

The Acting CHAIR. The unfinished business is the demand for a recorded vote on the amendment offered by the gentleman from Virginia (Mr. CONNOLLY) on which further proceedings were postponed and on which the ayes prevailed by voice vote.

The Clerk will redesignate the amendment.

The Clerk redesignated the amendment.

RECORDED VOTE

The Acting CHAIR. A recorded vote has been demanded.

A recorded vote was ordered.

The Acting CHAIR. This will be a 5-minute vote.

The vote was taken by electronic device, and there were—ayes 417, noes 4, not voting 18, as follows:

[Roll No. 38]

AYES—417

Abercrombie
Ackerman
Aderholt
Adler (NJ)
Akin
Alexander
Altmire
Andrews
Arcuri
Austria
Baca
Bachmann
Bachus
Baird
Baldwin
Barrow
Bartlett
Barton (TX)
Bean
Becerra
Berkley
Berman
Berry
Biggert
Bilbray
Bilirakis
Bishop (GA)
Bishop (NY)
Bishop (UT)
Blackburn
Blumenauer
Blunt
Boccieri
Boehner
Bonner
Bono Mack
Boozman
Bordallo
Boren
Boswell
Boucher
Boustany
Boyd
Brady (PA)
Brady (TX)
Braley (IA)
Bright
Brown (SC)
Brown, Corrine
Brown-Waite, Ginny
Buchanan
Burgess
Burton (IN)
Butterfield
Buyer
Calvert
Camp
Campbell
Cantor
Cao
Capito
Capps
Capuano
Cardoza
Carnahan
Carney
Carson (IN)
Carter
Cassidy
Castle
Chaffetz
Chandler
Childers
Chu
Clarke
Clay
Cleaver
Clyburn
Coble
Coffman (CO)
Cohen
Cole
Conaway
Connolly (VA)
Conyers
Cooper
Costa
Costello
Courtney
Crenshaw
Crowley
Cuellar
Culberson
Cummings
Dahlkemper
Davis (AL)
Davis (CA)
Davis (IL)
Davis (KY)
Davis (TN)
Deal (GA)
DeFazio
DeGette
Delahunt
DeLauro
Dent
Diaz-Balart, L.
Diaz-Balart, M.
Dicks
Dingell
Doggett
Donnelly (IN)
Doyle
Dreier
Driehaus
Duncan
Edwards (MD)
Edwards (TX)
Ehlers
Ellison
Ellsworth
Emerson
Engel
Eshoo
Etheridge
Faleomavaega
Fallin
Farr
Fattah
Filner
Fleming
Forbes
Fortenberry
Foster
Foxx
Frank (MA)
Franks (AZ)
Frelinghuysen
Fudge
Gallegly
Garamendi
Garrett (NJ)
Gerlach
Giffords
Gingrey (GA)
Gohmert
Gonzalez
Goodlatte
Gordon (TN)
Granger
Graves
Grayson
Green, Al
Green, Gene
Griffith
Grijalva
Guthrie
Hall (NY)
Hall (TX)
Halvorson
Hare
Harman
Harper
Hastings (FL)
Hastings (WA)
Heinrich
Heller
Hensarling
Herger
Herseth Sandlin
Higgins
Hill
Himes
Hinchey
Hinojosa
Hirono
Hodes
Hoekstra
Holden
Holt
Honda
Hoyer
Hunter
Inglis
Inslee
Israel
Issa
Jackson (IL)
Jackson Lee (TX)
Jenkins
Johnson (GA)
Johnson (IL)
Johnson, Sam
Jones
Jordan (OH)
Kagen
Kanjorski
Kaptur
Kennedy
Kildee
Kilpatrick (MI)
Kilroy
Kind
King (NY)
Kingston
Kissell
Klein (FL)
Kline (MN)
Kosmas
Kratovil
Kucinich
Lamborn
Lance
Langevin
Larsen (WA)
Larson (CT)
Latham
LaTourette
Latta
Lee (CA)
Lee (NY)
Levin
Lewis (CA)
Lewis (GA)
Linder
Lipinski
LoBiondo
Loebsack
Lofgren, Zoe
Lowey
Lucas
Luetkemeyer
Luján
Lummis
Lungren, Daniel E.
Lynch
Mack
Maffei
Maloney
Manzullo
Marchant
Markey (CO)
Markey (MA)
Marshall
Matheson
Matsui
McCarthy (CA)
McCarthy (NY)
McCaul
McCollum
McCotter
McDermott
McGovern
McHenry
McIntyre
McKeon
McMahon
McMorris Rodgers
McNerney
Meek (FL)
Meeks (NY)
Melancon
Mica
Michaud
Miller (FL)
Miller (MI)
Miller, Gary
Miller, George
Minnick
Mitchell
Mollohan
Moore (KS)
Moore (WI)
Moran (KS)
Moran (VA)
Murphy (CT)
Murphy (NY)
Murphy, Patrick
Murphy, Tim
Myrick
Nadler (NY)
Napolitano
Neal (MA)
Neugebauer
Norton
Nunes
Nye
Oberstar
Obey
Olson
Olver
Ortiz
Owens
Pallone
Pascrell
Pastor (AZ)
Paulsen
Payne
Pence
Perlmutter
Perriello
Peters
Peterson
Petri
Pierluisi
Pingree (ME)
Pitts
Platts
Poe (TX)
Polis (CO)
Pomeroy
Posey
Price (GA)
Price (NC)
Putnam
Quigley
Rahall
Rangel
Rehberg
Reichert
Reyes
Richardson
Rodriguez
Roe (TN)
Rogers (AL)
Rogers (KY)
Rogers (MI)
Rohrabacher
Rooney
Ros-Lehtinen
Roskam
Ross
Rothman (NJ)
Roybal-Allard
Royce
Ruppersberger
Ryan (OH)
Ryan (WI)
Sablan
Salazar
Sanchez, Loretta
Sarbanes
Scalise
Schakowsky
Schauer
Schiff
Schmidt
Schock
Schrader
Schwartz
Scott (GA)
Scott (VA)
Sensenbrenner
Serrano
Sessions
Sestak
Shadegg
Shea-Porter
Sherman
Shimkus
Shuler
Shuster
Simpson
Sires
Skelton
Smith (NE)
Smith (NJ)
Smith (TX)
Smith (WA)
Snyder
Souder
Space
Spratt
Stark
Stearns
Stupak
Sullivan
Sutton
Tanner
Taylor
Teague
Terry
Thompson (CA)
Thompson (MS)
Thompson (PA)
Thornberry
Tiahrt
Tiberi
Tierney
Titus
Tonko
Towns
Tsongas
Turner
Upton
Van Hollen
Velázquez
Visclosky
Walden
Walz
Wamp
Wasserman Schultz
Waters
Watson
Watt
Waxman
Weiner
Welch
Westmoreland
Whitfield
Wilson (OH)
Wittman
Wolf
Woolsey
Wu
Yarmuth
Young (AK)

NOES—4

Broun (GA)
Flake
McClintock
Paul

NOT VOTING—18

Barrett (SC)
Castor (FL)
Christensen
Gutierrez
Johnson, E. B.
King (IA)
Kirk
Kirkpatrick (AZ)
Massa
Miller (NC)
Murtha
Radanovich
Rush
Sánchez, Linda T.
Slaughter
Speier
Wilson (SC)
Young (FL)

ANNOUNCEMENT BY THE ACTING CHAIR

The Acting CHAIR (during the vote). Members are reminded there are 2 minutes left on this vote.

□ 1645

So the amendment was agreed to.

The result of the vote was announced as above recorded.

PERSONAL EXPLANATION

Mr. GUTIERREZ. Mr. Chairman, I was absent from the House Chamber today, due to a family emergency. Had I been present, I would have voted "aye" on rollcall votes 29, 30, 31, 32, 33, 34, 35, 36, 37, and 38.

Mr. MCGOVERN. Mr. Chairman, I move that the Committee do now rise.

The motion was agreed to.

Accordingly, the Committee rose; and the Speaker pro tempore (Mr. BRIGHT) having assumed the chair, Mr. PIERLUISI, 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. 4061) to advance cybersecurity research, development, and technical standards, and for other purposes, had come to no resolution thereon.

REPORT ON RESOLUTION PROVIDING FOR CONSIDERATION OF SENATE AMENDMENT TO H.J. RES. 45, INCREASING THE STATUTORY LIMIT ON THE PUBLIC DEBT

Mr. MCGOVERN, from the Committee on Rules, submitted a privileged report (Rept. No. 111–411) on the resolution (H. Res. 1065) providing for consideration of the Senate amendment to the joint resolution (H.J. Res. 45) increasing the statutory limit on the public debt, which was referred to the House Calendar and ordered to be printed.

JIM KOLBE POST OFFICE

(Ms. GIFFORDS asked and was given permission to address the House for 1 minute.)

Ms. GIFFORDS. Mr. Speaker, I rise today to commemorate the legacy of a former Member of Congress, Congressman Jim Kolbe. This body honors him with the passage of H.R. 4495, legislation to rename his hometown post office at 100 North Taylor Lane in Patagonia, Arizona.

Congressman Kolbe's record of service began as a page in this historic place of Congress for Senator Barry Goldwater. This experience would have a lasting impact on his appreciation for the virtue of public service, resulting in a long and distinguished career dedicated to cultivating a better Arizona, and in fact, a better Nation.

He spent his life in service in the United States Navy, the Arizona State legislature, and in the United States Congress for Arizona's Fifth and Eighth Congressional Districts. As our hometown newspaper, the Arizona Daily Star, noted upon his retirement in December of 2006, ''He earned a reputation as a moderate in a partisan world, a voice working from the center.''

Congressman Kolbe did not work from a predetermined list of party positions. He worked to unite his colleagues in finding solutions to important issues to Arizonans, from increased economic opportunity through trade to environmental conversation.

Mr. Speaker, I ask my colleagues to join with me in honoring this great figure, a man who served our community in Arizona, who served our Nation, Congressman Jim Kolbe, a true statesman and a beloved public figure.

COMMENDING PIUS BANNIS

(Ms. ROS-LEHTINEN asked and was given permission to address the House for 1 minute and to revise and extend her remarks.)

Ms. ROS-LEHTINEN. Mr. Speaker, I rise today to applaud the outstanding work and selfless commitment of Mr. Pius Bannis. Mr. Bannis is the Field Office Director in Port-au-Prince for the U.S. Citizenship and Immigration Services. He has gone above and beyond the call of duty in the weeks since the horrific earthquake that devastated Haiti on January 12.

Working around the clock, Mr. Bannis has helped to process hundreds of adoption cases, helping to unite American families with their Haitian children in the aftermath of this tragic disaster. Mr. Bannis is a hero. Because of his tireless efforts and compassion, many of the most vulnerable children in Haiti are able to look toward a much brighter future.

I am inspired by the selfless dedication, and again thank Mr. Bannis, as well as all of the employees of the U.S. Citizenship and Immigration Services, for their extraordinary service in helping Haitian children.

HONORING ANTONIO MANGLONA BORJA

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

Mr. SABLAN. Mr. Speaker, they say only the good die young. I don't know if only the good die young, but I do know that Antonio Manglona Borja from the island of Tinian in the Northern Mariana Islands was a very good man, and I do know that Antonia Manglona Borja has died much too young.

Tinian is a small island with a small number of families. Everyone knows everyone. And no one who lives there can fail to touch the lives of others. But some people have an impact on the community that is outsized, that makes their presence—and their absence—of greater significance.

Antonia Borja made his presence felt in so many ways: as an officer of the Department of Public Safety; as someone deeply involved with youth and adult sports; as a public representative on boards and commissions. Most of all, he was always there to give a hand to friends and neighbors in need.

Antonia Manglona Borja, Mr. Speaker. He was a good man. He died too young. And we all will miss him.

Mr. Speaker, They say only the good die young. I don't know if only the good die young. But I do know that Antonio Manglona Borja from the island of Tinian in the Northern Mariana Islands was a very good man. And I do know that Antonio Manglona Borja has died much too young.

So I rise today to honor him on the floor of the U.S. House of Representatives in the hope that knowing that Antonio was recognized in this way will give some comfort to his parents—Elias Manibusan Borja and Rosa Manglona Borja, to his wife—Bernadine Palacios Borja, to their children—Anthony Silvestre, Kristine, and Dennis—and to all Antonio's many friends and family members who miss him.

Mr. Speaker, Tinian is a small island with a small number of families. Everyone knows everyone. And no one who lives there can fail to touch the lives of others

But, of course, some people have an impact on the community that is outsize, that makes their presence—and their absence—of greater significance.

Antonio Borja made his presence felt in so many lives. As an officer of the Department of Public Safety, he helped to keep the peace on Tinian. He was there in moments of crisis and trauma for his community. He helped others and held them safe, when they were most in danger, most in need.

Mr. Borja learned the job of Public Safety Officer from the ground up, beginning as recruit in 1985 and quickly moving up the ranks to Captain in just nine years time. And Mr. Borja took what he learned as an officer and continued to contribute to the welfare of his community after his retirement nine years ago.

He was deeply involved with youth and adult sports. He served on the board of public corporations. Most of all, he was always there to give a hand to friends and neighbors in need.

Antonio Manglona Borja, Mr. Speaker. He was a good man. He died too young. And we all will miss him.

JUVENILE DIABETES

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

Mr. BOCCIERI. Mr. Speaker, I rise today in recognition of the 3 million young Americans who courageously fight juvenile diabetes every day. Recently, I had the privilege of meeting three brave children from my northeastern Ohio district, Andrew Butterworth, Meghan Jordan, and Gaetano Cecchini, who suffer from juvenile diabetes, but take their condition with great humility and strength.

Each day 40 children are diagnosed with diabetes in the United States. The price to maintain treatment can cost thousands of dollars per year. While insulin is enough to keep that person alive, it doesn't prevent the potential side effects of kidney failure, blindness, amputations, and heart attacks.