

fairly and enable the VA to set a standard for other Federal agencies. Mr. Speaker, the bill also makes several other improvements to the employment programs operated through the veterans employment and training service at the Department of Labor.

I am especially pleased that H.R. 3082 includes provisions of a bill I introduced to improve licensing and credentialing of veterans based on skills and experience they gained during their military service.

Mr. Speaker, in conclusion, this is an excellent bill. We need to pass it and make sure that the Senate gets the message loud and clear.

Mr. BUYER. I thank the gentlewoman for her contribution.

Mr. Speaker, I would now like to yield 2 minutes to the gentleman from Pennsylvania, the Honorable TIM MURPHY.

Mr. MURPHY. Mr. Speaker, this is a very important bill the House is now considering to extend a lot of critical services to veterans. I really on behalf of veterans am grateful for the work you have done on this.

Because of this type of bill, it cannot be amended, I would like to bring to your attention an issue that, Mr. Chairman, you and I have discussed, that we all remain very concerned about. That is the security breaches of veterans' personal records.

And if we are not able to pass a bill at this time, perhaps in the coming weeks or at least next year, we really need to be dealing with some of the issues, such as on November 2, a laptop containing 1,600 veterans records was stolen from a Manhattan hospital.

In August a desktop computer was stolen that had 38,000 veterans records, that had detailed records from the Pittsburgh and Philadelphia hospital areas.

Back in May we knew about another laptop computer that contained the personal records of 26 million veterans. I had introduced a bill, H.R. 6109, the Stop Endangering the Records of Veterans Act, or the SERV Act, in September which would require the VA to encrypt all data. I am pleased they are doing that now.

But we also need to have some teeth in this and make sure that those who do not properly protect veterans records, that there are penalties for them, criminal penalties if need be, if through their neglect or carelessness or direct action they cause a veteran's records to be stolen and cause harm from identity theft and just the problems that go with having medical records released.

Mr. Chairman, I am pleased that you are so concerned about these veterans issues. I don't know if there is time left in this session to deal with these issues. But I hope we can at the very least take this up in the next session. Veterans know that you, Mr. Chairman, have worked so diligently to protect them on so many issues. I look forward to continuing to work with

you on these issues, that we can work for our veterans' safety and peace of mind in the future.

Mr. FILNER. Mr. Speaker, I have no further speakers. I thank the chairman for bringing us this legislation of must-pass authorizations and extensions, and I yield back the balance of my time.

Mr. BUYER. Mr. Speaker, I yield myself the balance of our time.

Mr. Speaker, I thank Mr. FILNER for his cooperation on this bill and other bills. Mr. FILNER, we have got the CIO bill, we have got the cyber security bill. The Senate sent us two health bills, a benefit bill and we have got the construction bill. So all of these are in negotiation with the Senate. It is hard work. It represents 2 years of effort.

Recalling the recent words of my esteemed colleague, NANCY PELOSI, with the creation of this new theme of a bipartisan way for all Americans, let's embrace it. Let's get our work done. We enjoy bipartisanship on the Veterans' Affairs Committee, and I wish other committees could see how well we have worked together over the years. I call on leadership of everyone here in the House in dealing with these bills here on veterans affairs to complete our work on behalf of our Nation's veterans.

Mr. Speaker, I also call upon the Senate leadership to finish our legislative negotiations. Let's complete our work. Let's not forget our veterans and their families. And, Mr. Speaker, I also call upon the leadership of the veterans service organizations and the military service associations to encourage the Senate leadership to finish our negotiations and again finish the work that we had started on behalf of this Nation's veterans and dependents.

These warriors fought for our freedom. The least we can do is complete our work and provide for them the best care and benefits possible. Mr. Speaker, I urge my colleagues to support this bill.

Mr. MILLER of Florida. Mr. Speaker, I thank the chairman for bringing this bill to the floor today.

Included in H.R. 6314 is a provision to extend, through December 31, 2007, a program that provides government markers for veterans who are buried in a private cemetery.

The current five-year authority, which was effective for deaths that occurred as of September 11, 2001, expires on December 31st of this year.

Prior to this authority, if a veteran was buried at a private cemetery and the family purchased a private headstone, the veteran was ineligible for a government marker.

I want to recognize Representative NANCY JOHNSON, who has been championing this cause for over 5 years.

I appreciate her working with my Subcommittee to ensure that veterans and their families continue to have access to symbolic expressions of remembrance.

Mr. Speaker, as the 109th Congress comes to an end, I want to recognize Representative JEB BRADLEY, the Vice Chairman of the Subcommittee on Disability Assistance and Memo-

rial Affairs, and Ms. SHELLEY BERKLEY, the ranking member, for their active participation on the Subcommittee. We accomplished quite a bit over the past 2 years and I thank them both.

I also want to thank the Subcommittee staffs on both sides of the aisle—Paige McManus, Chris McNamee, and Mary Ellen McCarthy.

Finally, on behalf of the Subcommittee, I commend Chairman BUYER and Ranking Member EVANS for their bipartisan leadership of the House Committee on Veterans' Affairs.

Mr. Speaker, I urge my colleagues to support the bill before us.

Mr. BUYER. Mr. Speaker, I have no further requests for time, and I yield back the balance of my time.

The SPEAKER pro tempore (Mr. LAHOOD). The question is on the motion offered by the gentleman from Indiana (Mr. BUYER) that the House suspend the rules and pass the bill, H.R. 6314.

The question was taken.

The SPEAKER pro tempore. In the opinion of the Chair, two-thirds of those voting have responded in the affirmative.

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

The yeas and nays were ordered.

The SPEAKER pro tempore. Pursuant to clause 8 of rule XX and the Chair's prior announcement, further proceedings on this question will be postponed.

GENERAL LEAVE

Mr. BUYER. Mr. Speaker, I ask unanimous consent that Members may have 5 legislative days to revise and extend their remarks relative to the bill which the House just considered.

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

There was no objection.

□ 1200

EXPRESSING SENSE OF HOUSE WITH RESPECT TO RAISING AWARENESS AND ENHANCING THE STATE OF COMPUTER SECURITY

Mr. INGLIS of South Carolina. Mr. Speaker, I move to suspend the rules and agree to the resolution (H. Res. 993) expressing the sense of the House of Representatives with respect to raising awareness and enhancing the state of computer security in the United States, and supporting the goals and ideals of National Cyber Security Awareness Month.

The Clerk read as follows:

H. RES. 993

Whereas over 205,000,000 Americans use the Internet in the United States, including more than 84,000,000 home-users through broadband connections, to communicate with family and friends, manage their finances, pay their bills, improve their education, shop at home, and read about current events;

Whereas the approximately 26,000,000 small businesses in the United States, who represent 99.7 percent of all United States employers and employ 50 percent of the private

work force, increasingly rely on the Internet to manage their businesses, expand their customer reach, and enhance their connection with their supply chain;

Whereas according to the Department of Education, nearly 100 percent of public schools in the United States have Internet access, with approximately 93 percent of instructional rooms connected to the Internet, to enhance our children's education by providing access to educational online content and encouraging responsible self-initiative to discover research resources;

Whereas according to the Pew Institute, almost 9 in 10 teenagers between the ages of 12 and 17, or 87 percent of all youth (approximately 21,000,000 people) use the Internet, and 78 percent (or about 16,000,000 students) say they use the Internet at school;

Whereas teen use of the Internet at school has grown 45 percent since 2000, and educating children of all ages about safe, secure, and ethical practices will not only protect their systems, but will protect our children's physical safety, and help them become good cyber citizens;

Whereas the growth and popularity of social networking websites have attracted millions of teenagers, providing them with a range of valuable services, teens must be taught how to avoid potential threats like cyber bullies, predators and identity thieves they may come across while using such services;

Whereas our Nation's critical infrastructures rely on the secure and reliable operation of our information networks to support our Nation's financial services, energy, telecommunications, transportation, health care, and emergency response systems;

Whereas cyber security is a critical part of our Nation's overall homeland security, in particular the control systems that control and monitor our drinking water, dams, and other water management systems; our electricity grids, oil and gas supplies, and pipeline distribution networks; our transportation systems; and other critical manufacturing processes;

Whereas terrorists and others with malicious motives have demonstrated an interest in utilizing cyber means to attack our Nation, and the Department of Homeland Security's mission includes securing the homeland against cyber terrorism and other attacks;

Whereas Internet users and our information infrastructure face an increasing threat of malicious attacks through viruses, worms, Trojans, and unwanted programs such as spyware, adware, hacking tools, and password stealers, that are frequent and fast in propagation, are costly to repair, and disable entire systems;

Whereas according to Privacy Rights Clearinghouse, since February 2005, over 90 million records containing personally-identifiable information have been breached, and the overall increase in serious data breaches in both the private and public sectors are threatening the security and well-being of United States citizens;

Whereas consumers face significant financial and personal privacy losses due to identity theft and fraud, as reported in over 686,000 complaints in 2005 to the Federal Trade Commission's Consumer Sentinel database; and Internet-related complaints in 2005 accounted for 46 percent of all reported fraud complaints, with monetary losses of over \$680,000,000 and a median loss of \$350;

Whereas our Nation's youth face increasing threats online such as inappropriate content or child predators, according to the National Center for Missing and Exploited Children 34 percent of teens are exposed to unwanted sexually explicit material on the Internet, and with one in seven children hav-

ing been approached by a child predator on-line each year;

Whereas national organizations, policy-makers, government agencies, private sector companies, nonprofit institutions, schools, academic organizations, consumers, and the media recognize the need to increase awareness of computer security and enhance our level of computer and national security in the United States;

Whereas the National Cyber Security Alliance's mission is to increase awareness of cyber security practices and technologies to home users, students, teachers, and small businesses through educational activities, online resources and checklists, and Public Service Announcements; and

Whereas the National Cyber Security Alliance has designated October as National Cyber Security Awareness Month, which will provide an opportunity to educate the people of the United States about computer security: Now, therefore, be it

Resolved, That the House of Representatives—

(1) supports the goals and ideals of National Cyber Security Awareness Month; and

(2) will work with Federal agencies, national organizations, businesses, and educational institutions to encourage the development and implementation of existing and future computer security voluntary consensus standards, practices, and technologies in order to enhance the state of computer security in the United States.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from South Carolina (Mr. INGLIS) and the gentlewoman from California (Ms. MATSUI) each will control 20 minutes.

The Chair recognizes the gentleman from South Carolina.

GENERAL LEAVE

Mr. INGLIS of South Carolina. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days to revise and extend their remarks and to include extraneous materials on H. Res. 993, the resolution now under consideration.

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

There was no objection.

Mr. INGLIS of South Carolina. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I rise in support of H. Res. 993, a resolution to applaud the goals and activities of National Cyber Security Awareness Month.

Computers and the Internet have been integrated into our daily routine in businesses, schools and homes. These information and communication systems underpin our government, and they increase the productivity of our industries, financial institutions and transportation systems. However, our increasing dependence on computers and computer networks exposes our society to the risks of cyber attacks, destructive viruses, malicious hacking, and identity theft.

This is why the National Cyber Security Alliance, a cooperative effort between government, academia and industry, has organized National Cyber Security Awareness Month for each of the past 3 years and has already begun planning for the next National Cyber

Security Awareness Month in October 2007. As is only proper for a cyber security-related effort, there is a central Web site that is available all year round with on-line resources that offer tips and tools to help computer users protect themselves from viruses, worms, hacker attacks, identity theft, spyware and more.

In addition to these on-line resources, during National Cyber Security Awareness Month there are events all over the country on specific cyber security topics aimed at consumers, students, children, parents, small businesses and educational institutions. Attorneys general from 41 States and the District of Columbia have signed on to a resolution like H. Res. 993, supporting National Cyber Security Awareness Month. The National Cyber Security Alliance, in partnership with the Small Business Administration, sponsored a series of workshops to provide people from small businesses and nonprofit organizations with access to cyber security training developed by the National Institutes of Standards and Technology. In total, some sort of event on cyber security took place in 49 States during the month.

Of course, cyber security is not just an issue in October, but year round. National Cyber Security Awareness Month is a chance not only to raise awareness about computer vulnerabilities and threats, but also to inform people about programs that exist throughout the U.S. to educate students, parents, businesspeople, local law enforcement and government employees about cyber security and to attract students into careers in information technology.

For example, the National Science Foundation supports a program at the University of South Carolina in which undergraduates studying computer science and undergraduates training to be teachers team up on summer cyber security projects to get the experience of what actually doing research is like and to explore how the projects might be used to communicate about cyber security to K-12 students and to the general public.

In conclusion, I would like to thank Chairman LUNGREN, Ms. SANCHEZ, Chairman BOEHLERT, Mr. GORDON, Chairman KING and Mr. THOMPSON for introducing this resolution. We applaud the associations, companies, organizations and agencies involved in National Cyber Security Awareness Month for their efforts to help all of us to become more responsible, safer computer users.

I urge my colleagues to support adoption of the resolution.

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

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

Mr. Speaker, I rise in support of this resolution. It expresses congressional support for the goals and ideals of National Cyber Security Awareness Month.

This resolution, which I cosponsored, is an effort to increase awareness across the Nation of the dangers lurking in cyber space. It is also to educate Americans about the availability of tools and practices to minimize these dangers.

I want to congratulate the National Cyber Security Alliance for originating the idea for this observance and for its efforts to improve cyber security.

The National Cyber Security Alliance is a public/private partnership led by industry. It is focused on improving cyber security for home users, small businesses and educational institutions.

The Alliance seeks to alert computer users to threats such as viruses, hacking attacks and identity theft. Additionally, it provides information to users on best practices and technologies available for countering cyber threats.

Each year, nearly 10 million Americans are affected by identity theft, and it cost businesses almost \$56 billion in 2004. I frequently hear from my constituents in Sacramento about their experiences with identity theft and questions on how to avoid being a victim.

Consumer awareness has proven to be an effective weapon against identity theft, especially regarding Internet security. In fact, I received an overwhelmingly positive response when I hosted an information session on preventing identity theft in Sacramento.

National Cyber Security Awareness Month includes a range of special events designed specifically for home users, small businesses and the education community.

To reach its objectives, the Alliance organizes national and regional events. These events range from small business workshops and student assemblies to cyber security boot camps, which would take consumer education to the grass-roots level. The Alliance also makes public service announcements to inform consumers about on-line best practices and to protect their valuable personal data, and it publicizes its on-line resources for computer users. This includes beginner guides, computer security tips and free security scans.

The resolution before the House calls attention to and endorses the commendable efforts of the National Cyber Security Alliance to increase awareness of cyber security throughout the Nation. This is a message we should all heed.

Mr. Speaker, I commend this resolution to my colleagues and ask for their support for its passage by the House.

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

Mr. INGLIS of South Carolina. Mr. Speaker, I yield 4 minutes to the gentleman from California (Mr. DANIEL E. LUNGREN).

Mr. DANIEL E. LUNGREN of California. Mr. Speaker, I thank the gentleman for yielding, and I rise today in support the passage of House Resolu-

tion 993 to support the goals and ideals of National Cyber Security Awareness Month. This year, that month was in October, and while it is now November, I believe it is important to recognize the need for cyber security awareness not just in one month but throughout the entire year.

The Internet and the computers we use on a daily basis have become commonplace in our lives. Over 205 million Americans use the Internet on a regular basis, and that number is growing. Companies, both large and small, increasingly rely on the Internet and information technology systems to manage their business, expand their customer reach and enhance their connection with their supply chain.

With computers becoming less expensive and access to the Internet easier to accomplish, many dangers associated with on-line behavior are becoming more and more common. These threats range from spam, viruses and identity theft to complex computer attacks created by organized crime and terrorist organizations designed to steal personal financial information and create general havoc.

The Internet has become an invaluable tool in educating our children. Almost 90 percent of all youth use the Internet, and the vast majority of those say they use the Internet at school. As more and more children use the Internet, it is important that they are taught to use this tool in a safe, secure and ethical way. This will not only protect their own systems from attack, but will protect their physical safety and help them become good cyber citizens.

Cyber security is also a critical part of our Nation's overall homeland security. In particular, the control systems that control and monitor our drinking water, our dams and other water management systems, our electrical grids, oil and gas supplies, our transportation systems and other critical manufacturing processes are connected to the Internet. It is possible for terrorist organizations to disrupt a number of our critical infrastructure systems and do serious damage to our economy without even entering our country. Clearly, with much of the Nation's critical infrastructure connected to the Internet, appropriate cyber security practices are essential to our overall security.

It is not just terrorists that seek to do harm via computers and the Internet. More and more criminal activity is occurring in borderless cyber space. Through the Internet, international criminals can attack our computers through virus, worms and unwanted programs such as spyware and password stealers that can cause significant financial and personal privacy losses due to identity theft and fraud.

Organizations such as the National Cyber Security Alliance are making it their mission to increase awareness of cyber security practices and technologies to home users, students, teachers and small businesses. These

organizations deserve to be recognized for their good work and supported as much as possible to spread the awareness of good cyber security.

This organization's work is paying off. Cyber security awareness is growing. The Department of Homeland Security has recognized its importance by naming finally an Assistant Secretary for Cyber Security and Telecommunications, but there is much more work to be done. More government agencies, private sector companies, academic institutions, consumers and the media have to recognize the importance in establishing appropriate cyber security in their computers and information systems.

We, as a Congress, have a large role to play in encouraging the use of proper cyber security practices and technologies throughout our country. National Cyber Security Awareness Month provides a solid platform from which to improve cyber security awareness in this country, and I am pleased that this Congress is supporting its goals and ideals. As I have said, we have much work to do, but being aware of the need for cyber security is a necessary, essential first step.

I thank the gentleman for yielding.

Ms. MATSUI. Mr. Speaker, I yield 3 minutes to the gentlewoman from California (Ms. LORETTA SANCHEZ).

Ms. LORETTA SANCHEZ of California. Mr. Speaker, I thank my colleague from California for the time.

I rise in strong support of House Resolution 993 and the goals and ideals of the National Cyber Security Awareness Month, and I am proud to be one of the original cosponsors of this resolution.

I believe that raising awareness about the need to enhance computer and network security in the U.S. is a valuable tool to protect the identities and data of all Americans.

As the ranking member on the Economic Security, Infrastructure Protection and Cyber Security Subcommittee on the Committee on Homeland Security, I have had an opportunity to work on critical issues related to cyber security.

In the past, I have offered a number of amendments to various bills to increase our investment in cyber security research and development at the Department of Homeland Security, and I hope that in the next Congress we will make significant progress in this area.

I believe that we need to pay more attention to the state of cyber security because it affects all of us, from the government and large corporations to small businesses and, of course, to individuals.

Our country's infrastructure relies on secure information networks that ensure the reliable functioning of everything from public finance and control of water systems to the operation of electrical grids and emergency response systems.

For all of us, all Americans, our information infrastructure is an integral

part of our daily life, allowing us to communicate with friends and family, and pay bills and manage our business.

Imagine, if we go to the ATM and our money is gone, and this all leads back to some break in some network. At that point, we are going to realize just how important this is and how this can impact us on a daily basis.

It is the reliance on these information networks, these networks that are so much a part of our lives, and that is why it makes it such a great potential for targeted attacks by people who wish to harm us. And this type of attack would be devastating to our physical safety, as well as the economic security of our country. That is the reason I think that government needs to be a leader in the field of cyber security.

When I was talking to some of my companies about this, they said the simplest thing, about like over 50 percent of the people that use a network system do not use passwords. We should be using passwords. Those who use passwords may use something like the name of our dog or our pet; well, anybody who knows you can guess that or can get that name.

So I went through and I changed my passwords, and I changed Gretsky off of my passwords and everything else. Why? Because we need to. These are very simple, individual things that we can do because if once a person gets into the network, it goes much wider than that and can go into banking institutions and can go into the House of Representatives, et cetera.

□ 1215

So I urge my colleagues to support the goals and ideals of National Cyber Security Awareness Month. I hope every small business will take advantage of some of the free information with respect to making our networks safe.

Mr. BOEHLERT. Mr. Speaker, I rise in support of H. Res. 993, a resolution to applaud the goals and activities of National Cyber Security Awareness Month.

Information technology is becoming a critical part of our society, from wireless phones and blackberries to electronic medical records, and public trust in the security and reliability of these systems is necessary for the U.S. to realize the economic and societal benefits of new technologies.

Cybersecurity is also an important part of homeland security. The Science Committee has heard testimony from energy, electric power, and telecommunications companies about their dependence on information systems and their concerns about the nation's vulnerability to cyber attacks. The connectedness of the Internet means that each person not only must protect himself in cyberspace but also that each person's cybersecurity efforts contribute to the nation's overall state of cyber and homeland security. Progress is being made, but we as a Nation still have a long way to go.

Cybersecurity has long been a priority of mine, and I am proud to represent New York State, which has long been at the forefront of

developing new cybersecurity tools and training people in information security.

In my district, the Air Force's Rome Laboratory is a world leader in cybersecurity research programs to strengthen and protect the systems used by the military, and to develop forensic tools used by law enforcement at all levels. The laboratory also hosts innovative cybersecurity education programs including an annual Cyber Security Boot Camp to train ROTC cadets and civilian undergraduate students from all over the country in cutting edge cybersecurity techniques.

The Cyber Security Boot Camp has also led to the creation of a high school-level course in cybersecurity being taught at Rome Catholic High School in my district. This 20-week elective course will soon be accredited by the New York State Board of Education and can serve as a model for cybersecurity education nationwide.

As part of National Cyber Security Awareness Month, the University of Rochester hosted the 10-day Rochester Security Summit in collaboration with higher education, business and industry partners, and New York State ran a Poster Art Contest, open to all 4th and 5th grade students in the State, for art that illustrated how to use computers and the Internet safely.

I urge my colleagues to support adoption of H. Res. 993.

Ms. MATSUI. Mr. Speaker, I have no further requests for time, I urge passage of the resolution, and I yield back the balance of my time.

Mr. INGLIS of South Carolina. Mr. Speaker, I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from South Carolina (Mr. INGLIS) that the House suspend the rules and agree to the resolution, H. Res. 993.

The question was taken; and (two-thirds of those voting having responded in the affirmative) the rules were suspended and the resolution was agreed to.

A motion to reconsider was laid on the table.

GYNECOLOGIC CANCER EDUCATION AND AWARENESS ACT OF 2005

Mr. DEAL of Georgia. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 1245) to provide for programs to increase the awareness and knowledge of women and health care providers with respect to gynecologic cancers, as amended.

The Clerk read as follows:

H.R. 1245

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 "Gynecologic Cancer Education and Awareness Act of 2005" or "Johanna's Law".

SEC. 2. NATIONAL PUBLIC AWARENESS CAMPAIGN.

(a) IN GENERAL.—The Secretary of Health and Human Services (referred to in this Act as the "Secretary") shall carry out a national campaign to increase the awareness and knowledge of health care providers and women with respect to gynecologic cancers.

(b) WRITTEN MATERIALS.—Activities under the national campaign under subsection (a) shall include—

(1) maintaining a supply of written materials that provide information to the public on gynecologic cancers; and

(2) distributing the materials to members of the public upon request.

(c) PUBLIC SERVICE ANNOUNCEMENTS.—Activities under the national campaign under subsection (a) shall, in accordance with applicable law and regulations, include developing and placing, in telecommunications media, public service announcements intended to encourage women to discuss with their physicians their risks of gynecologic cancers. Such announcements shall inform the public on the manner in which the written materials referred to in subsection (b) can be obtained upon request, and shall call attention to early warning signs and risk factors based on the best available medical information.

SEC. 3. REPORT AND STRATEGY.

(a) REPORT.—Not later than 6 months after the date of the enactment of this Act, the Secretary shall submit to the Congress a report including the following:

(1) A description of the past and present activities of the Department of Health and Human Services to increase awareness and knowledge of the public with respect to different types of cancer, including gynecologic cancers.

(2) A description of the past and present activities of the Department of Health and Human Services to increase awareness and knowledge of health care providers with respect to different types of cancer, including gynecologic cancers.

(3) For each activity described pursuant to paragraph (1) or (2), a description of the following:

(A) The funding for such activity for fiscal year 2006 and the cumulative funding for such activity for previous fiscal years.

(B) The background and history of such activity, including—

(i) the goals of such activity;

(ii) the communications objectives of such activity;

(iii) the identity of each agency within the Department of Health and Human Services responsible for any aspect of the activity; and

(iv) how such activity is or was expected to result in change.

(C) How long the activity lasted or is expected to last.

(D) The outcomes observed and the evaluation methods, if any, that have been, are being, or will be used with respect to such activity.

(E) For each such outcome or evaluation method, a description of the associated results, analyses, and conclusions.

(b) STRATEGY.—

(1) DEVELOPMENT; SUBMISSION TO CONGRESS.—Not later than 3 months after submitting the report required by subsection (a), the Secretary shall develop and submit to the Congress a strategy for improving efforts to increase awareness and knowledge of the public and health care providers with respect to different types of cancer, including gynecological cancers.

(2) CONSULTATION.—In developing the strategy under paragraph (1), the Secretary should consult with qualified private sector groups, including nonprofit organizations.

SEC. 4. AUTHORIZATION OF APPROPRIATIONS.

For the purpose of carrying out this Act, there is authorized to be appropriated \$16,500,000 for the period of fiscal years 2007 through 2009.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from