TRIBUTE TO MRS. OLLYE BALLARD CONLEY OF HUNTSVILLE, ALABAMA

HON. ROBERT E. "BUD" CRAMER, JR.

OF ALABAMA

IN THE HOUSE OF REPRESENTATIVES

Tuesday, July 10, 2001

Mr. CRAMER. Mr. Speaker, I rise today to honor Mrs. Ollye Ballard Conley on her June 30th retirement after more than 35 years of dedicated service to the Huntsville City school system. Mrs. Conley has made the students of the Huntsville community shine through her creation of a top-notch magnet school, the Academy for Science and Foreign Language.

Her career in education is extensive and very impressive. Beginning as a teacher in Limestone County, Mrs. Conley has spent time teaching in Germany with the Department of Defense as well. After returning to Huntsville, her career took off and she soon rose through the ranks to become an administrator and then principal. She has led the schools of University Place, Rolling Hills and most recently the Academy for Science and Foreign Language to be more efficient, better organized schools. She believes in mission and her mission has been to provide the best environment possible for children to excel. She is innovative bringing in new curriculums such as the National Service-Learning program. The Academy is the only middle school in Alabama and only one of 34 nationwide to implement the service-learning program. She has shared her knowledge and the benefits of the service-learning program as a Regional Trainer for the Southern Region Corporation for National Service-Exchange.

Mrs. Conley believes that an education does not have to be limited to the classroom. Along with her students whom she inspires to achieve more and give back to their community, she established the first annual Community Day at Glenwood cemetery earning the Huntsville Historical Society Award and the Alabama Historical Commission Distinguished Service Award.

On behalf of the United States Congress and the people of North Alabama, I want to personally thank Mrs. Conley and pay tribute to her for her being an unsung hero. The difference she has made in countless children's lives over the years is incalculable. I would like to extend my best wishes to her, her family, friends and colleagues as they celebrate her well-deserved rest and a job well done.

INTRODUCTION OF THE CYBER SECURITY INFORMATION ACT OF 2001

HON. TOM DAVIS

OF VIRGINIA

IN THE HOUSE OF REPRESENTATIVES

Tuesday, July 10, 2001

Mr. TOM DAVIS of Virginia. Mr. Speaker, I am pleased to rise today to reintroduce legislation with my good friend and colleague from northern Virginia, Representative, JIM MORAN. Last year, we introduced H.R. 4246 to facilitate the protection of our nation's critical infrastructure from cyber threats. We aggressively pushed forward with the legislation and held a productive Subcommittee hearing with the then-Subcommittee on Government Management, Information, and Technology on the importance of the bill. Based on comments made at that hearing, we have worked hard with a wide range of industries to refine and improve this legislation. Today, we are again introducing this legislation with the full partnership of the private sector. Over the past several months, I have worked with the industry leaders from each of our critical infrastructure sectors to draft consensus legislation that will facilitate public-private partnerships to promote information sharing to prevent our nation from being crippled by a cyber-terrorism threat.

In the 104th Congress, we called upon the previous Administration to study our nation's critical infrastructure vulnerabilities and to identify solutions to address these vulnerabilities. Through that effort, a number of steps were identified that must be taken in order to eliminate the potential for significant damage to our critical infrastructure. Foremost among these suggestions was the need to ensure coordination between the public and private sector representatives of critical infrastructure. The bill we are again introducing today is the first step in encouraging private sector cooperation and participation with the government to accomplish this objective.

Since early spring of this year, Congress has held a number of hearings examining the ability of our nation to cope with cyber security threats and attacks. For instance, the House Energy and Commerce has held numerous hearings regarding the vulnerability of specific Federal agencies and entities, and how those agencies are implementing—or not implementing—the appropriate risk management tools to deal with these threats. The House Judiciary Subcommittee on Crime has held a number of hearings specifically looking at cybercrime from both a private sector and a federal law enforcement perspective. These hearings have demonstrated the importance of better, more efficient information sharing in protecting against cyber-threats as is encompassed in the legislation I have introduced today.

Also, the National Security Telecommunications Advisory Committee (NSTAC) met in early June of this year to discuss the necessary legislative action to encourage industry to voluntarily work in concert with the federal government in assessing and protecting against cyber vulnerabilities. The bill I am introducing today was endorsed at the June meeting. In recent months, the Bush Administration has aggressively been working with industry to address our critical infrastructure protection needs and ensure that the federal government is better coordinating its' cybersecurity efforts. I look forward in the coming weeks to working with the Administration to enhance the public-private partnership that industry and government must have in order to truly protect our critical infrastructure.

The critical infrastructure of the United States is largely owned and operated by the private sector. Critical infrastructures are those systems that are essential to the minimum operations of the economy and government. Our critical infrastructure is comprised of the financial services, telecommunications, information technology, transportation, water systems, emergency services, electric power, gas and oil sectors in private industry as well as our National Defense, and Law Enforcement and International Security sectors within the government. Traditionally, these sectors operated largely independently of one another and coordinated with government to protect themselves against threats posed by traditional warfare. Today, these sectors must learn how to protect themselves against unconventional threats such as terrorist attacks, and cyber intrusions.

These sectors must also recognize the vulnerabilities they may face because of the tremendous technological progress we have made. As we learned when planning for the challenges presented by the Year 2000 rollover, many of our computer systems and networks are now interconnected and communicate with many other systems. With the many advances in information technology, many of our critical infrastructure sectors are linked to one another and face increased vulnerability to cyber threats. Technology interconnectivity increases the risk that problems affecting one system will also affect other connected systems. Computer networks can provide pathways among systems to gain unauthorized access to data and operations from outside locations if they are not carefully monitored and protected.

A cyber threat could quickly shutdown any one of our critical infrastructures and potentially cripple several sectors at one time. Nations around the world, including the United States, are currently training their military and intelligence personnel to carry out cyber attacks against other nations to quickly and efficiently cripple a nation's daily operations. Cyber attacks have moved beyond the mischievous teenager and are now being learned and used by terrorist organizations as the latest weapon in a nation's arsenal. During this past spring, around the anniversary of the U.S. bombing of the Chinese embassy in Belgrade, U.S. web sites were defaced by hackers, replacing existing content with pro-Chinese or anti-U.S. rhetoric. In addition, an Internet worm named ''Lion'' infected computers and installed distributed denial of service (DDOS) tools on various systems. An analysis of the Lion worm's source code revealed that it could send password files from the victim site to e-mail address located in China.

We have learned the inconveniences that may be caused by a cyber attack or unforeseen circumstance. Last year, many of individuals and companies were impacted by the ''I Love You'' virus as it moved rapidly around the world disrupting the daily operations of many of our industry sectors. The Love Bug showed the resourcefulness of many in the private sector in identifying and responding to such an attack but it amply demonstrated the weakness of the government's ability to handle such a virus. Shortly after the attack, Congress learned that the U.S. Department of Health and Human Services' (HHS) operating systems were so debilitated by the virus that it could not have responded adequately if we had faced a serious public health crisis at the same time. Additionally, the federal government was several hours behind industry in notifying agencies about the virus. If the private sector could share information with the government within a defined framework, federal agencies could have been made aware of the threat earlier on.

Last month, NIPC and FedCIRC received information on attempts to locate, obtain control of and plant new malicious code known as ''W32-Leaves.worm'' on computers previously

infected with the SubSeven Trojan. SubSeven is a Trojan Horse that can permit a remote computer to gain complete control of an infected machine, typically by using Internet Relay Chat (IRC) channels for communications. In June 1998 and February 1999, the Director of the Central Intelligence Agency testified before Congress that several nations recognize that cyber attacks against civilian computer systems represent the most viable option for leveling the playing field in an armed crisis against the United States. The Director also stated that several terrorist organizations believed information warfare to be a low cost opportunity to support their causes. We must, as a nation, prepare both our public and private sectors to protect ourselves against such efforts.

That is why I am again introducing legislation that gives critical infrastructure industries the assurances they need in order to confidently share information with the federal government. As we learned with the Y2K model, government and industry can work in partnership to produce the best outcome for the American people. Today, the private sector has established many information sharing organizations (ISOs) for the different sectors of our nation's critical infrastructure. Information regarding a cyber threat or vulnerability is now shared within some industries but it is not shared with the government and it is not shared across industries. The private sector stands ready to expand this model but have also expressed concerns about voluntarily sharing information with the government and the unintended consequences they could face for acting in good faith. Specifically, there has been concern that industry could potentially face antitrust violations for sharing information with other industry partners, have their shared information be subject to the Freedom of Information Act, or face potential liability concerns for information shared in good faith. My bill will address all three of these concerns. The Cyber Security Information Act also respects the privacy rights of consumers and critical infrastructure operators. Consumers and operators will have the confidence they need to know that information will be handled accurately, confidentially, and reliably.

The Cyber Security Information Act is closely modeled after the successful Year 2000 Information and Readiness Disclosure Act by providing a limited FOIA exemption, civil litigation protection for shared information, and an antitrust exemption for information shared among private sector companies for the purpose of correcting, avoiding, communicating or disclosing information about a cyber-security related problem. These three protections have been requested by the U.S. Chamber of Commerce, the National Association of Manufacturers, the Edison Electric Institute, the Information Technology Association of America, Americans for Computer Privacy, and the Electronics Industry Alliance. Many private sector companies have also asked for this important legislation. I have attached to my statement a letter from the many professional associations and private sector companies supporting the introduction of this measure.

This legislation will enable the private sector, including ISOs, to move forward without fear from the government so that government and industry may enjoy a mutually cooperative partnership. This will also allow us to get a timely and accurate assessment of the vulnerabilities of each sector to cyber attacks and allow for the formulation of proposals to eliminate these vulnerabilities without increasing government regulation, or expanding unfunded federal mandates on the private sector.

ISOs will continue their current leadership role in developing the necessary technical expertise to establish baseline statistics and patterns within the various infrastructures, as clearinghouses for information within and among the various sectors, and as repositories of valuable information that may be used by the private sector. As technology continues to rapidly improve industry efficiency and operations, so will the risks posed by vulnerabilities and threats to our infrastructure. We must create a framework that will allow our protective measures to adapt and be updated quickly.

It is my hope that we will be able to move forward quickly with this legislation and that Congress and the Administration will work in partnership to provide industry and government with the tools for meeting this challenge. A Congressional Research Service report on the ISOs proposal describes the information sharing model as one of the most crucial pieces for success in protecting our critical infrastructure, yet one of the hardest pieces to realize. With the introduction of the Cyber Security Information Act of 2001, we are removing the primary barrier to information sharing between government and industry. This is landmark legislation that will be replicated around the globe by other nations as they too try to address threats to their critical infrastructure.

Mr. Speaker, I believe that the Cyber Security Information Act of 2001 will help us address critical infrastructure cyber threats with the same level of success we achieved in addressing the Year 2000 problem. With government and industry cooperation, the seamless delivery of services and the protection of our nation's economy and well-being will continue without interruption just as the delivery of services continued on January 1, 2000.

JULY 5, 2001.

Hon. ——
U.S. House of Representatives,
Washington, DC

DEAR REPRESENTATIVE: We, the undersigned, representing every sector of the United States economy, write today to strongly urge you to become an original cosponsor of the Cyber Security Information Act to be shortly introduced by Representatives Tom Davis and Jim Moran. This important bill will strengthen information sharing legal protections that shield U.S. critical infrastructures from cyber and physical attacks and threats.

Over the past four years, industry-government information sharing regarding vulnerabilities and threats has been a key element of the federal government's critical infrastructure protection plans. Several industry established information sharing organizations, including Information Sharing and Analysis Centers (ISACs) and the Partnership for Critical Infrastructure Security (PCIS), have been set up to support this initiative. The National Plan for Information Systems Protection, version 1.0, also calls for private sector input about actions that will facilitate industry-government information sharing.

As representative companies and industry associations involved in supporting the ongoing development of a National Plan for critical infrastructure protection, we believe that Congress can play a key role in facilitating this initiative by passing legislation to support the Plan's strategic objectives.

Currently, there is uncertainty about whether existing law may expose companies and industries that voluntarily share sensitive information with the federal government to unintended and potentially harmful consequences. This uncertainty has a chilling effect on the growth of all information sharing organizations and the quality and quantity of information that they are able to gather and share with the federal government. As such, this situation is an impediment to the effectiveness of both industry and government security and assurance managers to understand, collaborate on and manage their vulnerability and threat environments.

Legislation that will clarify and strengthen existing Freedom of Information Act and antitrust exemptions, or otherwise create new means to promote critical infrastructure protection and assurance would be very helpful and have a catalytic effect on the initiatives that are currently under way.

Companies in the transportation, telecommunications, information technology, financial services, energy, water, power and gas, health and emergency services have a vital stake in the protection of infrastructure assets. With over 90 percent of the country's critical infrastructure owned and/or operated by the private sector, the government must support information sharing between the public and private sectors in order to ensure the best possible security for all our citizens. A basic precondition for this cooperation is a clear legal and public policy framework for action.

Businesses also need protection from unnecessary restrictions placed by federal and state antitrust laws on critical information sharing that would inhibit identification of R&D needs or the identification and mitigation of vulnerabilities. There are a number of precedents for this kind of collaboration, and we believe that legislation based on these precedents will also assist this process.

Faced with the prospect of unintended liabilities, we also believe that any assurances that Congress can provide to companies voluntarily collaborating with the government in risk management planning activity—such as performing risk assessments, testing infrastructure security, or sharing certain threat and vulnerability information—will be very beneficial. Establishing liability safeguards to encourage the sharing of threat and vulnerability information will add to the robustness of the partnership and the significance of the information shared.

Thank you for considering our views on this important subject. We think that such legislation will contribute to the success of the institutional, information-sharing, technological, and collaborative strategies outlined in Presidential Decision Directive—63 and version 1.0 of the National Plan for Information Systems Protection.

Sincerely,
Americans for Computer Privacy.
Edison Electric Institute.
Fannie Mae.
Internet Security Alliance.
Information Technology Association of America.
Microsoft.
National Center for Technology and Law, George Mason University.
Owest Communications.
Security.
Computer Sciences Corporation.
Electronic Industries Alliance.
The Financial Services Roundtable.
Internet Security Systems.
National Association of Manufacturers.
Mitretek Systems.
The Open Group.

Oracle.
U.S. Chamber of Commerce.

WHY INFORMATION SHARING IS ESSENTIAL FOR CRITICAL INFRASTRUCTURE PROTECTION

FREQUENTLY ASKED QUESTIONS

What are Critical Infrastructures?

Critical Infrastructures are those industries identified in Presidential Decision Directive—63 and version 1.0 of the National Plan for Information Systems Protection, deemed vital for the continuing functioning of the essential services of the United States. These include telecommunications, information technology, financial services, oil, water, gas, electric energy, health services, transportation, and emergency services.

What Is the Problem?

90% of the nation's critical infrastructures are owned and/or operated by the private sector. Increasingly, they are inter-connected through networks. This has made them more efficient, but it has also increased the vulnerability of multiple sectors of the economy to attacks on particular infrastructures. According to the Carnegie-Mellon Computer Emergency Response Team (CERT), cyber attacks on critical infrastructures have grown at an exponential rate over the past three years. This trend is expected to continue for the foreseeable future. In our free market system, it is not feasible to have a centralized-government monitoring function. A voluntary national industry-government information sharing system is needed in order for the nation to create an effective early warning system, find and fix vulnerabilities, benchmark best practices and create new safety technologies.

How Do Industries and the Government Share Information?

Based on PDD–63 and the National Plan, a number of organizations have been created to foster industry-government cooperation. These include Information Sharing and Analysis Centers (ISACs). ISACs are industry-specific and have been set up in the financial services, telecommunications, IT, and electric energy industries. Others are in the process of being organized. ISACs vary in their membership structures and relationship to the government. Most of them have a formal government sector liaison as their principal point of contact.

What Are Current Concerns?

Companies are concerned that information voluntarily shared with the government that reports on or concerns corporate security may be subject to FOIA. They are also concerned that lead agencies may not be able to effectively control the use or dissemination of sensitive information because of similar legal requirements. Access to sensitive information may fall into the hands of terrorists, criminals, and other individuals and organizations capable of exploiting vulnerabilities and harming the U.S. Unfiltered, unmediated information may be misinterpreted by the public and undermine public confidence in the country's critical infrastructures. Also, competitors and others may use that information to the detriment of a reporting company, or as the basis for litigation. Any and all of these possibilities are reasons why the current flow of voluntary data is minimal.

What Can Be Done?

Possible solutions include creating an additional exemption to current FOIA laws. There are currently over 80 specific FOIA Exemptions throughout the body of U.S. law, so it is clear that exempting voluntarily shared information that could affect national security is consistent with the intent and application of FOIA. Another solution is to build on existing relevant legal precedents such as the 1998 Y2K Information and Readiness Disclosure Act, the 1984 National Cooperative Research Act, territorially limited court rulings, and individual, advisory Department of Justice Findings.

Why Pursue a Legislative Solution?

The goal is to provide incentives for voluntary information sharing. Legislation can add legal clarity that will provide one such incentive, as well as also demonstrate the support and commitment of Congress to increasing critical infrastructure assurance.

PERSONAL EXPLANATION

HON. SHELLEY BERKLEY

OF NEVADA

IN THE HOUSE OF REPRESENTATIVES

Tuesday, July 10, 2001

Ms. BERKLEY. Mr. Speaker, flight delays caused me to miss rollcall votes Nos. 186, 187, and 188. Had I been present, I would have voted "yes" on No. 186, "yes" on No. 187, and "yes" on No. 188.

CELEBRATING THE DEFENSE LOGISTICS AGENCY'S 40TH ANNIVERSARY

HON. JAMES P. MORAN

OF VIRGINIA

IN THE HOUSE OF REPRESENTATIVES

Tuesday, July 10, 2001

Mr. MORAN of Virginia. Mr. Speaker, I rise today to congratulate the Defense Logistics Agency's 40th anniversary. The Defense Logistics Agency has a distinguished history as the nation's combat support agency. Its origins date back to World War II when America's entrance into the global conflict required the rapid procurement of large amounts of munitions and supplies. When the agency was first founded, managers were appointed from each branch of the armed services for this task. In 1961, the Department of Defense centralized management of military logistics support by establishing the Defense Supply Agency. After 16 years of increasing responsibilities, the Defense Supply Agency expanded its original charter and was renamed the Defense Logistics Agency in 1977.

I would like to commend the Defense Logistics Agency's impeccable record of supporting defense and humanitarian missions. It stands as a testament to the agency's commitment to provide seamless support of our armed forces around the world and to extend a helping hand to victims of all types of adversity.

As the world has changed and evolved, the Defense Logistics Agency also has adapted and proven its ability to streamline. Agency employees have shown dedication to improving quality, reducing costs and improving responsiveness to their warfighter customer needs. They have also demonstrated their ability to embrace the latest technologies of today's competitive business world, which has resulted in saving the taxpayers billions of dollars. The Defense Logistics Agency's record of achievement serves as an example of government service at its best, highlighted by two Joint Meritorious Service Awards.

On behalf of my colleagues, I would like to praise the individual efforts of the men and women involved in the Defense Logistics Agency, and thank them for making the Agency a world-class organization. In honor of the 40th anniversary of the Defense Logistics Agency, we are proud of the Defense Logistics Agency's past endeavors and look forward to a bright and successful future of continued commitment and service to our nation.

Mr. Speaker, I ask you to join me in extending congratulations and best wishes to the employees of the Defense Logistics Agency on this memorable occasion and achievement.

TRIBUTE TO JAMES H. MULLEN

HON. MARION BERRY

OF ARKANSAS

IN THE HOUSE OF REPRESENTATIVES

Tuesday, July 10, 2001

Mr. BERRY. Mr. Speaker, I rise today to pay tribute to a great Arkansan and outstanding educator. I am proud to recognize James H. Mullen in the Congress for his invaluable contributions and service to his community, to our state, and to our nation.

For over three decades James Mullen of DeWitt, Arkansas has made a profound impact on the lives of people. Born in Mendenhall, Mississippi, James served in the United States Air Force during World War II. After being honorably discharged, he used the GI benefits to attend Mississippi State University, where he earned a degree in agriculture. That government investment would reap tremendous returns.

After graduating from Mississippi State, James moved to DeWitt, an area primarily dependent on its agrarian strengths. It was his responsibility to assist other veterans in developing their agricultural proficiency.

In 1955, James accepted a job with the DeWitt Independent School system teaching agriculture. For the next eleven years he would remain in this position. His influence far exceeded his teaching responsibilities.

It was not uncommon for young men to seek him out for personal counsel. His home was always open to young men who needed a listening ear, wise counsel, or any type of support. On one occasion a former student came to James and informed him he was going to quit college because of lack of funds. Although James didn't have the money to loan the student, he did the next best thing and went to the bank and secured a personal loan.

Each summer, in addition to visiting in the home of each student, James would take a group of students to camp. He had the unique ability to have fun with the students while maintaining an authoritarian position. On one visit to summer camp, the students destroyed his hat. With James, there were two things you never messed with: his hat or his pipe! Before nightfall, he had driven all those boys to town and required them to purchase a new hat. He never lost control!

In 1966, James joined the Arkansas State Department of Education as Associate Director of Petit Jean Vocational Technical School in Morrilton, Arkansas. He would remain in that position until 1970 when he was named Director of the Crowley's Ridge Vocational Technical School in Forrest City, Arkansas. At Crowley's Ridge, he inherited a fledgling institution and successfully restored the integrity of the institution.

Construction of the Rice Belt Vocational Technical School was approved in 1974. Community leaders from DeWitt would accept no