with the 9th Marines in Vietnam. Near the end of his tour of duty, his unit was near the Rock Pile in the Northern Eye Core of Vietnam when a mortar round landed between Mr. Conely and another soldier. The other man was thrown 23 feet and killed, while Mr. Conely ended up with shrapnel throughout his body.

A third generation soldier whose grandfather served in World War I and his father in World War II, Mr. Conely's wounds sadly forced him to leave the military. He had planned to make a career in the Marines, but after the blast injured him in Vietnam he returned to Bethesda Naval Hospital where he remained for 13 months prior to being discharged. Continuing the tradition of military service, Mr. Conely's three sons have all served in the Marine Corps, and one has had four tours of duty in Iraq.

Madam Speaker, it is soldiers like Thomas S. Conely, Sr., who joined the military to protect the freedoms that all Americans hold dear. While brave men like Mr. Conely were wounded fighting for freedom and liberty, his family, friends and loved ones know that this Congress will always remember his bravery and commitment in battle.

INTRODUCTION OF THE TAX RELIEF FOR TRANSPORTATION WORKERS ACT

HON. RON PAUL

OF TEXAS

IN THE HOUSE OF REPRESENTATIVES

Wednesday, May 7, 2008

Mr. PAUL. Madam Speaker, I rise to introduce the Tax Relief for Transportation Workers Act. This legislation helps those who work in the port industry cope with the costs of complying with Congress's mandate that all those working on a port obtain a Transportation Worker Identity Card (TWIC). The Tax Relief for Transportation Workers Act provides a tax credit to workers who pay the costs of obtaining TWICs. The credit is refundable against both income and payroll tax liabilities. This legislation also provides a tax deduction for businesses that pay for their employees to obtain a TWIC.

When Congress created the TWIC requirement, it placed the burden of paying the cost of obtaining the card on individual workers. Imposing the costs of obtaining TWICs on port workers has several negative economic impacts that Congress should help mitigate by making the cost associated with obtaining a TWIC tax deductible. According to the Department of Homeland Security, a port worker will have to pay between $100 and $132 dollars to obtain a card. The worker will also have to pay a $60 fee for every card that is lost or damaged. Even those employers whose employers pay the substantial costs of obtaining TWICs for their workforce are adversely affected by the TWIC requirement, as the money employers pay for TWICs is money that cannot go into increasing their workers' salaries. The costs of the TWIC requirement may also cause some employers to refrain from hiring new employees.

Ironically, many of the employees whose employers are unable to pay the TWIC are part-time or temporary workers at the lower end of the income scale. Obviously, the TWIC requirement hits these workers the hardest. According to Recana, an employer of port workers in my district, the fee will have a ''significant impact'' on port workers.

Unless Congress acts to relieve some of the economic burden the TWIC requirement places on those who work in the port industry, the damage done could reach beyond the port employers and employees to harm businesses that depend on a strong American port industry. This could be very harmful to both interstate and international trade.

Regardless of what one thinks of the merits of the TWIC card, it is simply not right for Congress to make the port industry bear all the costs of TWIC. I therefore urge my colleagues to stand up for those who perform vital tasks at America's ports by cosponsoring the Tax Relief for Transportation Workers Act.

SUPPORT FOR THE COPPER-BASE CASTING TECHNOLOGY PROGRAM

HON. JOE WILSON

OF SOUTH CAROLINA

IN THE HOUSE OF REPRESENTATIVES

Wednesday, May 7, 2008

Mr. WILSON of South Carolina. Madam Speaker, I wish to express my strong support for the Copper-Base Casting Technology Program, C–BCT, a program of great importance to the people of South Carolina, as well as the men and women serving in the United States military at home and overseas. The C–BCT program is a cooperative relationship between the copper industry and the Department of Defense, working to apply high-performance copper alloys in military applications.

Since it's inception in 2004, the C–BCT program has provided multiple, breakthrough technologies for defense and industrial systems that have benefits for all branches of the military. Advances include the design and creation of prototype high-efficiency induction motors using copper rotors. Copper rotors increase motor energy efficiency, lower manufacturing costs due to reductions in overall materials used, increase motor life, and reduce motor weight and size. C–BCT provides the military a technology that has produced crucial advances for the American war-fighter in land base, shipboard, and aerospace applications and has done so in a cost-effective manner.

I would like to recognize Daniel Gearing with the Defense Logistics Agency, DLA, for his support and oversight of the launching of C–BCT. In addition, Victor Champagne with the Army Research Lab, ARL, has begun advanced work to apply C–BCT in applications that advance the defense community requirements. The applications are driven by the need for higher efficiency, lighter weight, lower cost, environmentally friendly, and more reliable materials. Reduced weight, in particular, is a common goal for all weapon systems and logistics support items. With DLA and ARL's commitment to continue the success of C–BCT, advances to date may soon be brought to our service men and women serving overseas. Together with the Copper Development Association and the Advanced Technology Institute, these organizations are working to demonstrate and evaluate copper's ultimate potential for our military.

I recognize the crucial benefits that C–BCT offers both the domestic copper industry and the U.S. armed services as well as the successes of the current program and the critical nature of copper in most military applications.

INTRODUCTION OF THE HOMELAND SECURITY NETWORK DEFENSE AND ACCOUNTABILITY ACT OF 2008

HON. JAMES R. LANGEVIN

OF RHODE ISLAND

IN THE HOUSE OF REPRESENTATIVES

Wednesday, May 7, 2008

Mr. LANGEVIN. Madam Speaker, today we are introducing the Homeland Security Network Defense and Accountability Act of 2008, a bill designed to improve the cybersecurity posture of the Department of Homeland Security.

The security of our federal and critical infrastructure networks is an issue of national security. The United States and its allies face a significant and growing threat to our information technology, IT, systems and assets, and to the integrity of our information. The acquisition of our government's information by outsiders undermines our strength as a nation and over time could cost the United States our advantage over our adversaries. This is a critical issue that we can no longer ignore.

One of the first things that Chairman THOMPSON tasked me with when I was named Chairman of the Subcommittee on Emerging Threats, Cybersecurity and Science and Technology was to lead a bipartisan inquiry into the cybersecurity posture of our federal networks and our critical infrastructure. Viewing the potential for cyber attacks on federal networks as an emerging threat that warrants attention, Chairman THOMPSON challenged me to address the four areas that the 9/11 Commission determined our systems failed: in imagination, policy, capabilities, and management. The same can be said of the federal government's approach to cybersecurity—and as a result, our critical information and technology systems are vulnerable to cyber terrorists.

So far in the 110th Congress, we have held seven hearings on cybersecurity, heard from hundreds of experts on how best to tackle this issue, reviewed information security best practices in the public and private sectors, investigated cyber incidents across the spectrum, from the State and Commerce Departments to our Nation's electric grid, and uncovered and assisted law enforcement in investigating breaches at the Department of Homeland Security. It has become clear that an organization is only as strong as the integrity and reliability of the information that it keeps. Therefore we must make cybersecurity a national priority.

This legislation represents a small but critical step toward improving the cybersecurity posture at the Department of Homeland Security by addressing two key issues: ensuring a robust defense-in-depth of our information systems, and holding individuals at all levels accountable for mitigating vulnerabilities. Early in our investigative process, I announced that the Committee's oversight goals were to increase public awareness of the problems associated with federal network security; fix those vulnerabilities that are, or could be, successfully exploited; and hold individuals, agencies, and private sector entities responsible for their

actions. Though much work remains to be done, I believe that we are moving in the right direction. The Department has already begun acting to improve its information security as a result of several Committee hearings. By fully implementing and carefully considering the intent of this bill, I believe the Department of Homeland Security will continue to make great strides in improving its information security posture. I hope that one day DHS will be considered a global leader in cybersecurity.

This measure is comprised of several important pieces. First, this bill would establish authorities and qualifications for the Chief Information Officer, CIO, position at the Department of Homeland Security. In March 2007, Secretary Chertoff issued a management directive giving the Chief Information Officer hiring authority for CIOs and approval authority over agency CIO budgets and IT investments. This bill statutorily authorizes that directive, but includes additional requirements for information security qualifications. In a number of hearings, we expressed concern that the lack of an information security background can hamper the CIO's understanding and efforts to secure the Department's networks. We cannot allow future Presidents to repeat the mistakes made by this Administration in appointing unqualified individuals to this important office.

This bill would also establish specific operational security practices for the CIO, including a continuous, real-time cyber incident response capability, a network architecture emphasizing the positioning of security controls, and vulnerability assessments for each external-facing information infrastructure. As we learned through our investigations of cyber incidents on DHS networks, the absence of a 24 hour/7 day a week real-time response capability can lead to devastating consequences, and we simply cannot afford significant time lapses in our response to cyber incidents.

This legislation also includes testing protocols to reduce the number of vulnerability exploitations throughout the Department's networks. Through our investigations and oversight hearings, we identified a significant gap between requirements under the Federal Information Security Management Act, FISMA, and the current threat environment. As we have learned, agencies that receive high FISMA scores are not necessarily secure from the latest attacks. This provision will require the CIO to consult with other federal agencies and establish attack-based testing protocols to secure Department networks. Today, one of the biggest problems with FISMA is that while we continue to identify vulnerabilities in our systems, we fail to provide adequate funding to mitigate those vulnerabilities. This bill will hold both the CIO and the agency head responsible for developing and implementing a vulnerability mitigation plan that includes budget and personnel marks.

The ubiquitous nature of the Internet can lead to significant problems if one party is infected with a virus or rootkit that can penetrate another person's network undetected. That is why our bill requires the Secretary to determine if the internal security policy of a contractor who provides network services to the Department matches the requirements of the Department. Network service providers for the Department are also required to implement and regularly update their internal information security policies, and deliver timely notice of any computer incidents that could affect the Department's computers. This section is similar to provisions contained in the security controls developed by the National Institute of Standards and Technology, NIST, special condition ''SA–9.''

Finally, we seek a formal report from the Secretary on several critical issues. I was disturbed to learn that the Department still has not conducted a risk assessment on its unclassified network, despite a series of breaches, and we seek a detailed counter-intelligence plan from the Secretary to investigate all breaches, as well as an outline of a program to increase threat information sharing with cleared contractors. DHS must also examine a similar undertaking, and consider offering training to contractors using the attack-based protocols established in consultation with the defense and intelligence communities. We also ask the Secretary to update us on how effective the Department has been in meeting the deadlines established by the Office of Management and Budget, OMB, for Trusted Internet Connections, TIC, encryption and authentication mandates.

Regrettably, poor information security practices plague the entire federal government, not just DHS. NIST continues to serve as an excellent guide for robust cybersecurity practices; unfortunately, federal agencies are often quick to cut cybersecurity budgets in favor of tangible products. If we care about information security, then we must not allow agencies to bleed money out of these programs.

Of course, legislation alone will not accomplish our goals. The Homeland Security Committee continues to conduct robust oversight over this Administration's Cyber Initiative. While I support the aim of the Cyber Initiative, I continue to have significant questions about the scope, budget, and secrecy of these efforts. Furthermore, there are several critical issues that each federal agency must immediately address to improve its security posture. We must start conducting robust damage assessments that can measure exposure to current attacks, and continue to fix those vulnerabilities. We must enhance and educate the federal workforce to limit successful exploits. We must support focused R&D efforts to solve the big challenges that face us in the world of cybersecurity. We must support and enhance initiatives like the Federal Desktop Core Configuration, the OMB-mandated security configuration for all Microsoft Windows Vista and XP operating system software. We must continue to monitor the efforts of the Administration to collapse federal connections to the Internet, known as the TIC Initiative. And finally, we must hold accountable those responsible for these efforts—whether they are our CIOs or Chief Information Security Officers, OMB, DHS, the Defense Department, the Intelligence community or contractors charged with securing our networks. Information security must become a prime concern for each of us if we are to ever be successful in defending ourselves from attack.

Madam Speaker, the Homeland Security Network Defense and Accountability Act of 2008 is a robust and carefully crafted bill, and is the result of a bipartisan effort to treat information security and cybersecurity with the same attention and effort that our adversaries would use to exploit us. I thank Chairman THOMPSON for co-sponsoring this bill with me, and I send the bill to the desk and ask that it be properly referred to the Homeland Security Committee.

RICHARD WIDMARK AND THE SPIRIT OF TEXAS

HON. TED POE

OF TEXAS

IN THE HOUSE OF REPRESENTATIVES

Wednesday, May 7, 2008

Mr. POE. Madam Speaker, the Spirit of Texas has been a popular genre in the classic Westerns of Hollywood. Recently, Hollywood and Texas lost Richard Widmark, who starred as Jim Bowie in the 1960 John Wayne version of The Alamo. Widmark's portrayal of Bowie is a classic representation of the fire that drove the defenders of the Alamo and soldiers of Texas to secure their independence.

John Wayne's version of The Alamo does more than just tell a story. Characters attach themselves to the audience. Richard Widmark did just that in his role as Jim Bowie. The contrast between the liberal minded Widmark and the conservative John Wayne is one of the highlights of the movie, and illustrates that the defenders of the Alamo came from all different backgrounds and mindsets. More importantly, however, is that Widmark and his fellow cast members captivated audiences with the Spirit of Texas and the devotion the defenders had in sacrificing their lives for their country. Widmark himself captures this spirit near the end of the movie, when he fights to the death with his famous Bowie Knife as he is lamed up in bed.

Richard Widmark recently passed away at his home in Roxbury, Connecticut on March 24. While not a Texan by birth, his contribution to the movies and the story of the defenders of the Alamo is one that should be remembered. His portrayal of Jim Bowie is a testament to the Spirit of Texas and her citizens. As we ''Remember The Alamo,'' we should also ''Remember Richard Widmark.''

IN HONOR OF THE AZERBAIJANI CULTURAL GARDEN

HON. DENNIS J. KUCINICH

OF OHIO

IN THE HOUSE OF REPRESENTATIVES

Wednesday, May 7, 2008

Mr. KUCINICH. Madam Speaker, and colleagues, I rise today in recognition of the grand opening of the Azerbaijani Cultural Garden on May 12, 2008.

The Azerbaijani Garden is part of the Cleveland Cultural Gardens along Doan Brook in Cleveland's Rockefeller Park. I strongly support the addition of the Azerbaijani Garden as part of the Cleveland Cultural Gardens Federation and all the international communities represented through its gardens.

The Cleveland Cultural Gardens date back to 1916 when the Shakespeare Garden was built. By 1926, the concept of a series of gardens, recognizing various nationalities, was established. The formal group was completed in 1939 with funding to a large degree provided by the federal government. At that time, a series of 18 gardens was dedicated to the City of Cleveland, symbolizing the fusion of distinct nationalities into one American culture.

More importantly, these gardens stood for the brotherhood among all the people of all nations and to this day remain a unique embodiment of that purpose. On July 30, 1939,