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