He was appointed by then Gov. David Pryor to the State Board of Corrections for a five-year term. He was appointed by then Gov. Bill Clint- ton to the Arkansas Agriculture Museum Board in Scott and he, along with Governor Clinton and State Rep. Bill Foster were instrumen- tial in securing funding for this preserva- tion project for the farming community of Scott. "This," as said by William, "is a project that is very dear to me." William was a life-long member of All Souls Church in Scott. He has served as Sunday School Superintendent, Chairman of the church Board of Directors, and as All Souls Church Trustee until the age of 75. Sadly, William died last month. He was pre- ceded in death by one son, Judge Don Bevis of Cabot, and he is survived by his wife of 58 years, Mary Jo Bennett Bevis, two sons—Rep. Bill Davis, Jr. and his wife Kay of Scott and Bob Bevis and his wife Liz of Scott—along with numerous grandchildren and great-grand- children and a host of friends. On behalf of the Congress, I extend sym- pathies and condolences to the family of Wil- liam Jackson Bevis, Sr. His name commands respect and honor from all who knew him.

TRIBUTE TO MRS. OLLYE
BALLARD CONLEY OF HUNTS- VILLE, 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 Hunts- ville, 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 re- cently the Academy for Science and Foreign Language to be more efficient, better orga- nized schools. She believes in mission and her mission has been to provide the best envi- ronment 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 commu- nity, she established the first annual Commun- ity Day at Glenwood cemetery earning the

INTRODUCTION OF THE CYBER SE- CURITY 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 legis- lation with my good friend and colleague from Northern Virginia, Mr. Jim Moran. Last year, we introduced H.R. 4246 to facili- tate the protection of our nation’s critical infra- structure from cyber threats. We aggressively pushed forward with the legislation and held a productive Subcommittee hearing with the then-Subcommittee on Government Manage- ment, Information, and Technology on the im- portance 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 intro- ducing this legislation with the full partnership of the private sector. Over the past several months, I have worked with the industry lead- ers from each of our critical infrastructure sec- tors to draft consensus legislation that will fa- cilitate 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 en- sure coordination between the public and pri- vate sector representatives of critical infra- structure. 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 on the vulnerability of specific Federal agencies and entities, and how those agencies are implementing—or not imple- menting—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 encom- passed in the legislation I have introduced today.

Also, the National Security Telecommuni- cations Advisory Committee (NSTAC) met in early June of this year to discuss the nec- essary 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 in- troducing today was endorsed at the June meeting. In recent months, the Bush Adminis- tration has aggressively been working with in- dustry to address our critical infrastructure pro- tection needs and ensure that the federal gov- ernment is better coordinating its’ cybersecurity efforts. I look forward in the coming weeks to working with the Administra- tion to enhance the public-private partnership that industry and government must now enter 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 op- erations of the economy and society. Our critical infrastructure is comprised of the finan- cial 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 gov- ernment. Traditionally, these sectors operated largely independently of one another and co- ordinated with government to protect them- selves against threats posed by traditional warfare. Today, these sectors must learn how to protect themselves against unconventional threats such as terrorist attacks, and cyber in- trusions.

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 roll- over, many of our computer systems and net- works are now interconnected and commu- nicate with many other systems. With the many advances in information technology, many of our critical infrastructures are now linked to one another and face increased vul- nerability to cyber threats. Technology interconnectivity increases the risk that prob- lems affecting one system will also affect other connected systems. Computer networks can provide pathways among government systems to allow unauthorized access to data and operations from outside locations if they are not carefully mon- itored and protected.

A cyber threat could quickly shutdown any one of our critical infrastructures and poten- tially cripple several sectors at one time. Na- tions around the world, including the United States, are currently training their military and intelligence personnel to carry out cyber at- tacks against other nations to quickly and effi- ciently cripple a nation’s daily operations.

Cyber attacks have moved beyond the mis- chievous teenager and are now being learned and used by terrorist organizations as the lat- est weapon in a nation’s arsenal. During this past spring, around the anniversary of the