

Mr. Speaker, Frank began his illustrious career when he started his own hay bailing business at the age of 14. Through his vision and entrepreneurial spirit he was able to establish a successful family farm operation. He and his wife, Susan, today run a heifer replacement operation and grow alfalfa, corn and barely in southeastern Idaho.

When Frank is not busy on the farm, he, Susan and their 6 children attend church and actively participate in youth group activities. Clearly, we are fortunate to have someone like Frank serve the people of Idaho, and I personally want to wish him a heartfelt thanks for his dedicated service.

HONORING GREEK INDEPENDENCE DAY

HON. DEBBIE STABENOW

OF MICHIGAN

IN THE HOUSE OF REPRESENTATIVES

Wednesday, April 12, 2000

Ms. STABENOW. Mr. Speaker, I rise today to honor the 179th Greek Independence Day. On March 25, 1821, the Greek people started a battle that would lead to independence after more than 400 years of Ottoman rule.

Fortunately, Greek culture survived the Ottomans. Greek civilization inspired the framers of our constitution. The Greek political tradition had profound influence on our founding fathers and helped shape America's political foundation. The pursuit of freedom is just one of the many ideals which have historically bound us together.

Greek-Americans have made such a enormous contribution to American culture and American life. Today, Greek culture flourishes in America—in places like Detroit, Michigan and elsewhere in the Great Lakes States.

As a member of the Congressional Caucus on Hellenic Issues, I want to take this opportunity to salute the Greek people on their historic achievement. Greece is a dedicated U.S. ally.

I congratulate Greece for 179 years of independent rule and for a legacy that will last forever. My fellow colleagues, please join me in honoring Greek Independence Day.

HONORING THE LEXINGTON LIONS CLUB FOR 79 YEARS OF SERVICE TO THE COMMUNITY

HON. ERNIE FLETCHER

OF KENTUCKY

IN THE HOUSE OF REPRESENTATIVES

Wednesday, April 12, 2000

Mr. FLETCHER. Mr. Speaker, I acknowledge the accomplishments of an outstanding organization within the community of Lexington, Kentucky. With a motto of "We Serve", the Lexington Lions Club has been serving folks in the Lexington community for the past 79 years.

Its members always give freely of their time and labor to serve our nation, our state and local community. Their dedication to the ideals of service and high standards promotes good citizenship and the welfare of our neighborhoods. The members of the Lexington Lions have worked tirelessly to produce positive change and as a result, their efforts have helped many over the years.

I believe their hard work and dedication is obvious, as the Lexington Lions Club will come together on Friday, April 28, 2000 to celebrate its "Million Dollar Decade". Since 1990, this organization has worked to raise the necessary funds to serve the needs of our community. Their efforts to prevent blindness and their dedication to serving young people have touched and improved the lives of so many—I salute this remarkable organization for its many achievements, accomplishments and years of dedicated service.

Mr. Speaker, today I recognize an outstanding organization that has made so many contributions throughout its 79 years of service. It is an honor to share with my colleagues and the American people how the Lexington Lions Club has constantly given to make Lexington and Kentucky a better place.

IN SUPPORT OF METHAMPHETAMINES LEGISLATION

HON. MARY BONO

OF CALIFORNIA

IN THE HOUSE OF REPRESENTATIVES

Wednesday, April 12, 2000

Mrs. BONO. Mr. Speaker, it is time to declare war against methamphetamines. Meth is a powerful and dangerous drug that harms innocent families and ruins neighborhoods and communities.

This dangerous drug is a threat to our society and our prosperity and it is time we take responsibility for solving this problem.

I rise to support Congressman CALVERT's legislation that will ensure that law enforcement officials are fully equipped with the resources to battle this destructive drug.

Meth has become the drug of choice in California and in my district. Worse, it is easy to manufacture and acquire. In fact, in Fiscal Year 1999, there were over 700 meth labs seized in Riverside and San Bernardino counties alone at a cost of \$1.3 million dollars to taxpayers.

Many anti-government forces believe that the war on drugs is a failure and that we should stop the fight. As a concerned parent, I strongly believe that it is our responsibility to not run and hide, but rather to step up to the plate and increase our commitment to the war against drugs. This legislation represents this continued commitment.

HONORING TORRANCE CITY COUNCIL MEMBERS HARVEY HORWICH, DON LEE, AND MAUREEN O'DONNELL

HON. STEVEN T. KUYKENDALL

OF CALIFORNIA

IN THE HOUSE OF REPRESENTATIVES

Wednesday, April 12, 2000

Mr. KUYKENDALL. Mr. Speaker, I rise today to honor three distinguished individuals from the City of Torrance, Council members Harvey Horwich, Don Lee, and Maureen O'Donnell. Today they are being honored for their service to the community as their tenure on the City Council comes to an end.

All three individuals have exhibited a strong commitment to the local community. They have extensively volunteered their time for the

betterment of the community. I commend their selfless contributions to the City of Torrance.

Councilman Horwich has been an active volunteer in the community for over 20 years. He has been involved with the Torrance Civic Center Authority, the Parks and Recreation Commission, and the Planning Commission. A local small businessman, Harvey was appointed to the City Council in November of 1998.

A lifelong resident of the South Bay, Councilman Lee was first elected to the City Council in 1992. Prior to his service on the Council, Don Lee was a Planning Commissioner and a Parks and Recreation Commissioner for the City of Torrance. He is actively involved in the Torrance Rotary Club, YMCA, and Chamber of Commerce.

Councilwoman O'Donnell is a standout educator, teacher of American government and U.S. History at Gardena High School. She has been active in local politics and served on the Torrance Human Resources commission prior to her election to the City Council in 1992. She was selected as the Torrance YWCA Woman of the Year in 1994, and has been involved with the Torrance Historical Society, YWCA, and the Salvation Army.

Council members Horwich, Lee, and O'Donnell have been invaluable members of the Torrance community. On behalf of the City of Torrance, I thank you for your service. You have served the Torrance community with respect and honor.

INTRODUCTION OF THE CYBER SECURITY INFORMATION ACT OF 2000

HON. THOMAS M. DAVIS

OF VIRGINIA

IN THE HOUSE OF REPRESENTATIVES

Wednesday, April 12, 2000

Mr. DAVIS of Virginia. Mr. Speaker, I am pleased to rise today to introduce legislation with my good friend and colleague from northern Virginia, Representative JIM LORAN, that will facilitate the protection of our nation's critical infrastructure from cyber threats. In the 104th Congress, we called upon the Administration to study our nation's critical infrastructure vulnerabilities and to identify solutions to address these vulnerabilities. The Administration has, through the President and participating agencies, identified a number of steps that must be taken in order to eliminate the potential for significant damage to our critical infrastructure. Foremost among these suggestions is the need to ensure coordination between the public and private sector representatives of critical infrastructure. The bill I am introducing today is the first step in encouraging private sector cooperation and participation with the government to accomplish this objective.

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 attack. 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 being learned and used by terrorist organizations as the latest weapon in a nation's arsenal. 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. Both Presidential Decision Directive 63 (PDD-63) issued in May 1998, and the President's National Plan for Information Systems Protection, Version 1.0 issued in January 2000, call on the legislative branch to build the necessary framework to encourage information sharing to address cyber security threats to our nation's privately held critical infrastructure.

Recently, we have learned the inconveniences that may be caused by a cyber attack or unforeseen circumstance. Earlier this year, many of our most popular sites such as Yahoo, eBay and Amazon.com were shutdown for several hours at a time over several days by a team of hackers interested in demonstrating their capability to disrupt service. While we may have found the shutdown of these sites temporarily inconvenient, they potentially cost those companies significant amounts of lost revenue, and it is not too difficult to imagine what would have occurred if the attacks had been focused on our utilities, or emergency services industries. We, as a society, have grown increasingly dependent on our infrastructure providers. I am sure many of you recall when PanAmSat's Galaxy IV satellite's on-board controller lost service. An estimated 80 to 90% of our nation's pagers

were inoperable, and hospitals had difficulty reaching doctors on call and emergency workers. It even impeded the ability of consumers to use credit cards to pay for their gas at the pump.

Moreover, recent studies have demonstrated that the incidence of cyber security threats to both the government and the private sector are only increasing. According to an October 1999 report issued by the General Accounting Office (GAO), the number of reported computer security incidents handled by Carnegie-Mellon University's CERT Coordination Center has increased from 1,334 in 1993 to 4,398 during the first two quarters of 1999. Additionally, the Computer Security Institute reported an increased in attacks for the third year in a row based on responses to their annual survey on computer security. GAO has done a number of reports that give Congress an accurate picture of the risk facing federal agencies; they cannot track such information for the private sector. We must rely on the private sector to share its vulnerabilities with the federal government so that all of our critical infrastructures are protected.

Today, I am 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. The President has called for the creation of Information Sharing and Analysis Centers (ISACs) for each critical infrastructure sector that will be headed by the appropriate federal agency or entity, and a member from its private sector counterpart. For instance, the Department of Treasury is running the first ISAC for the financial services industry in partnership with Citigroup. Many in the private sector have expressed strong support for 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 of 2000 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 within an ISAC. These three protections have been previously cited by the Administration as necessary legislative remedies in Version 1.0 of the National Plan and PDD-63. This legislation will enable the ISACs to move forward without fear from industry so that government and industry may enjoy the mutually cooperative partnership called for in PDD-63. 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.

PDD-63 calls upon the government to put in place a critical infrastructure proposal that will allow for three tasks to be accomplished by 2003:

(1) The Federal Government must be able to perform essential national security missions and to ensure the general public health and safety;

(2) State and local governments must be able to maintain order and to deliver minimum essential public services; and

(3) The private sector must be able to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial, and transportation services. This legislation will allow the private sector to meet this deadline.

We will also ensure the ISACs can move forward to accomplish their missions by developing the necessary technical expertise to establish baseline statistics and patterns within the various infrastructures, become a clearinghouse for information within and among the various sectors, and provide a repository 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 can move forward in partnership to provide industry and government with the tools for meeting this challenge. A Congressional Research Service report on the ISAC proposal describes the information sharing model 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 2000, 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 2000 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.

COMMEMORATING THE DAY OF
HONOR 2000 FOR AMERICA'S
MINORITY VETERANS OF WORLD
WAR II

HON. LANE EVANS

OF ILLINOIS

IN THE HOUSE OF REPRESENTATIVES

Wednesday, April 12, 2000

Mr. EVANS. Mr. Speaker, I join with many of my colleagues today to honor and give thanks to America's minority veterans—the