EXTENSIONS OF REMARKS

INITIAL VICTORY IN THE STRUGGLE FOR FREEDOM OF THE PRESS IN RUSSIA—BUT THE FIGHT MUST GO ON

HON. TOM LANTOS

OF CALIFORNIA

IN THE HOUSE OF REPRESENTATIVES

Thursday, July 27, 2000

Mr. LANTOS. Mr. Speaker, in the long and difficult fight for freedom of the press in Russia we have won an important victory today. The Russian prosecutor informed Vladimir Gusinsky—head of Russia's Media-Most media conglomerate—that the case against him has been dropped for "the lack of a fact of a crime."

Mr. Speaker, the prosecutor's action against Mr. Gusinsky was never simply a case of prosecuting a crime. From the beginning it has been a case of seeking to persecute and harass and intimidate and muzzle the free press in Russia. Vladimir Gusinsky is the head of Media-Most, which owns NTV television network, Russia's leading independent television network, as well as Echo of Moscow radio, and a number of other important independent media ventures.

It is significant, Mr. Speaker, that NTV and other Media-Most journalists have been critical of Russian President Putin and of the actions of the Russian government. Critical journalism is certainly nothing that would even raise eyebrows in the United States or Western Europe or other free countries around the world.

Mr. Speaker, the harassment of Mr. Gusinsky involved actions against him that go well beyond what would be done in a normal criminal proceeding involving such charges. Mr. Gusinsky was jailed for four days in June; in a high-handed fashion authorities seized documents from his company's offices several times; after he was released from jail, he was repeatedly called in for questioning; he was prohibited from traveling abroad; and steps were taken to freeze his personal assets.

On a number of occasions in the past, I have called to the attention of my colleagues in this House the systematic efforts to harass and intimidate the independent media in Russia. I hope that President Putin now understands that there is no room for Russia in the community of free and democratic nations if his government engages in efforts to oppress and threaten the free press in Russia.

Mr. Speaker, the dropping of charges against Mr. Gusinsky represents a victory for democracy and press freedom in Russia, but the battle is far from over. We must continue and strengthen our efforts to preserve free media in Russia.

INTRODUCTION OF THE FEDERAL INFORMATION POLICY ACT OF 2000

HON. THOMAS M. DAVIS

OF VIRGINIA

IN THE HOUSE OF REPRESENTATIVES

Thursday, July 27, 2000

Mr. DAVIS of Virginia. Mr. Speaker, I rise today to introduce legislation that will endow the Federal Government with the ability to better coordinate and manage information technology policies governmentwide and transform the Federal Government into a national model for information resources management and information security practices. The Federal Information Policy Act [FIPA] of 2000 establishes an Office of Information Policy with a Chief Information Officer [CIO] for the United States and creates within that body, an Office of Information Security and Technical Protection [IN STEP]. This legislation harmonizes existing information resources management responsibilities now held by OMB and provides IN STEP with the responsibility for facilitating the development of a comprehensive, federal framework for devising and implementing effective, mandatory controls over government information security. In this latter respect, the Act is the logical complement to legislation I introduced in April, the Cyber Security Information Act of 2000, which seeks to encourage private sector information sharing with government in order to protect our national critical infrastructure. The Federal Information Policy Act will force the Federal Government to put its house in order and become a reliable public partner for protecting America's information highways.

For nearly four decades, information technology has been an integral component of information resources management [IRM] by the Federal Government. The Government's role as the single largest procurer of IT products and services in the 1960s and 1970s spurred the development of the U.S. computer industries that now form the backbone of our nation's New Economy. A decade ago, technology stood as one of many factors important to the mission and performance objectives of the Federal Government. Now both our economy and our society have become information-driven, such that IT plays the critical role in facilitating the Federal Government's ability to be effective and efficient in managing federal programs and spending, communicating with and providing services to citizens, and protecting America's critical infrastructure.

Five years ago, Congress recognized the crucial role played by technology when we called on the Administration to appoint a top-level officer to focus exclusively on the Year 2000 computer problem that threatened to undermine national commerce and government. This determination—that a single individual was needed to coordinate national and local cooperation to remediate computer systems and develop contingency plans—was based in part on an understanding of the interconnectivity of information systems within government, between government and the private sector, and within the private sector. The President heeded our recommendation and appointed John Koskinen to a Cabinet-level position as the chairman of the President's Council on Year 2000 Conversion.

Moreover, the Year 2000 computer problem highlighted two important deficiencies in the current Federal IRM structure. First, the Y2K scenario presented an important reminder that technology does not fill some amorphous role within the Federal Government. It is the ubiquitous thread that binds the operations of the Federal Government, and its efficient or inefficient use will make or break the ability of government to perform everything from the most mundane of governmental functions to the most critical national security measures. Second, the high degree of interdepence between information systems, both internally and externally, exposes the vulnerability of the Federal Government's computer networks to both benign and destructive disruptions. This factor is tremendously important to understanding how we devise a comprehensive and flexible strategy for coordinating, implementing and maintaining federal information security practices throughout the Federal Government as the rising threat of electronic terrorism emerges.

In following the lessons learned from the Y2K problem as well as the recent Love Bug viruses that affected many federal computer systems, the Federal Information Policy Act accomplishes four main purposes: (1) to revise chapter 35 of title 44 of the U.S. Code to establish a Federal Chief Information Officer to head the Office of Information Policy (OIP) within the Executive Office of the President; (2) to consolidate and centralize IRM powers currently allotted to the Office of Management and Budget [OMB] within the OIP; (3) to establish within the OIP the Office of Information Security and Technical Protection [IN STEP]; and (4) to establish a comprehensive framework implementing mandatory information security standards, and annual independent evaluations of agency practices in order to provide effective controls over Federal information resources. The Act creates a new chapter 36 to retain OMB's paperwork clearance functions that are currently contained in chapter 35 and are performed by the Office of Information and Regulatory Affairs.

This past May, at the Center for Innovative Technology in my congressional district, the House Government Reform Subcommittee on Government Management, Information, and Technology held a hearing in which we explored the strategies and challenges facing government in implementing electronic government initiatives. We learned that while electronic government initiatives promise to provide faster, more efficient, and convenient services, the Internet sets forth a wide array of challenges that must be addressed in order for the lower costs and improved customer service associated with electronic government to be realized. These include theft, fraud, consumer privacy protection, and the destruction

of assets. To meet those challenges, the General Accounting Office [GAO] testified that "effective top management leadership, involvement, and ownership are a cornerstone of any information technology investment strategy."

The Paperwork Reduction Act [PRA] established the Office of Information and Regulatory Affairs [OIRA] within OMB and gave the Office the authority to reduce unnecessary paperwork burdens and to "develop and maintain a Governmentwide strategic plan for information resources management." However, in a July 1998 report, the GAO found that OIRA had failed to satisfy some of its IRM responsibilities assigned by the PRA. And last year, the GAO found that improvements in broad IT management reforms "will be difficult to achieve without effective agency leadership support, highly qualified and experienced CIOs, and effective OMB leadership and oversight."

I am deeply concerned that current federal IRM policies are suffering from the lack of a focused, coordinating body. The Clinger-Cohen Act, passed in the 104th Congress, made an important contribution to Federal IT policy by mandating that federal agencies appoint Chief Information Officers and by recognizing the need to coordinate and facilitate interagency IT communication and policies, a role given to OMB. But having each agency develop IT policies independently of one another poses the potential risk of having a government unable to communicate and function and function amongst its own parts. A central IT management process is essential if government is going to be able to successfully achieve cost benefits similar to those experienced in the private sector and improve its responsiveness to the public through e-government initiatives and better-performing Federal operations. And that coordinating entity must be capable of deploying comprehensive policies that reflect the interdependence of federal information systems.

With its many management responsibilities, OMB is simply unable to devote the attention need for effective IRM. FIPA creates a CIO of the United States to fulfill that coordinating role, acting as the principal adviser to the President on the development, application and management of information technology government-wide. He or she will be able to encourage innovation in technology uses, coordinate inter-agency IRM initiatives and communication, and promote cost-effective investments in information technologies. The Act also formalizes the establishment of the Chief Information Officers Council, which currently exists by virtue of a 1996 Executive Order. Made up of the CIOs from the major Federal agencies, the CIO Council provides an important forum for interagency communication and for improving IT management policies, procedures, and standards. The Federal CIO will chair the Council, a position now held by the Deputy Director for Management at OMB, and must submit an annual report to the President and Congress on its achievements and recommendations for future initiatives.

A Federal CIO will allow OIRA to concentrate and improve on the critical function of paperwork reduction that is so important to our continued efforts to minimize bureaucratic burdens on individuals, small businesses, and others resulting from the collection of information by or for the Federal Government. It is for this reason that the paperwork clearance functions are maintained in FIPA.

Equally critical is the ability of the Federal Government to anticipate, monitor, and recover from intrusions into Federal computer networks. This important objective was detailed in the President's National Plan for Information Systems Protection, Version 1.0, issued in January 2000. Many sectors of the government have experienced, at one time or another, cyber security breaches. Under current law, rules and regulations governing the security of federal computer systems are guided by the Computer Security Act of 1987 and Annex III of OMB Circular A–130. The result is that several agencies including OMB, the National Institute of Standards and Technology [NIST], the General Services Administration, and the National Security Agency, all play a role in overseeing and implementing computer security procedures and reviews. Cyber security readiness is an intrinsic element of every information resources management. But like Federal IRM policy in general, the integrity of Federal information systems is being endangered by a lack of government-wide coordination and implementation of proven information security practices.

Certainly, each Federal agency must bear the responsibility for assessing risk, detecting and responding to security incidents, and protecting its own operations and assets. It is for this reason that this legislation also adapts many of the provisions contained in the Government Information Security Act championed by Senate Governmental Affairs Committee Chairman FRED THOMPSON. It requires every Federal agency to develop and implement security policies that include risk assessment, risk-based policies, security awareness training, and periodic reviews.

However, in a March 2000 Senate hearing on the Government Information Security Act, the GAO pointed to compelling reasons for establishing strong central leadership for coordinating information security-related activities across government. Foremost is the inadequacy of information-sharing among agencies regarding vulnerabilities and solutions to those weaknesses, as well as the lack of a clear mandate for handling and reporting security incidents affecting federal information systems.

For instance, in a March 29, 2000 hearing, the House Government Reform Subcommittee on Government Management, Information and Technology examined the state of information security practices throughout the Federal Government. GAO shared its most recent review at that time of the Environmental Protection Agency [EPA]. Its tests found "numerous security weaknesses associated with the computer operating systems and the agencywide computer network that support most of EPA's mission-related and financial operations." Indeed, the EPA had recorded several serious computer incidents within the last two years but the GAO indicated that EPA's subsequent methods for strengthening its security procedures were inadequate. In an earlier report, the GAO stated that "resolving EPA's information security problems will require substantial ongoing management attention since security program planning and management to date have largely been a paper exercise doing little to substantively identify, evaluate, and mitigate risks to the agency's data and systems."

As part of its testimony, the GAO referred to earlier findings that 22 of the largest federal agencies were providing inadequate protection for critical federal operations and assets from

computer-based attacks. GAO reported that within the past year, it was able to identify systemic weaknesses in the information security practices of the Department of Defense, the National Aeronautics and Space Administration, the Department of State, and the Department of Veterans Affairs. In each instance, sensitive data and/or mission-critical systems were penetrable by unauthorized users.

These results reflect government-wide systemic weaknesses and follow numerous GAO audits which have repeatedly identified serious failures in the most basic access controls for Federal information systems. In its May 1999 tests of NASA's computer-based controls, GAO was able to successfully gain access to several mission-critical systems, and could have easily disrupted command and control operations conducted through orbiting spacecraft. An independent auditor found last August that the State Department's mainframe computer was extremely vulnerable to unauthorized access that could expose, in turn, other computer operations connected to those mainframe computers. These are just a few examples of the many troubling indicators that currently plague Federal agency information security practices.

Another key challenge to making the Federal Government more secure lies in the mind set of many federal agencies vis-a-vis the importance of information security to their operations and assets. For many, implementing best practices for controlling and protecting information resources is a low priority. A centralized leader would be able to make information security one of the top priority missions of the Federal Government. It is this overarching responsibility that is given to the United States CIO in the Act, and is subsequently delegated to the Director of IN STEP. In establishing government-wide policies, the IN STEP Director will direct the implementation of a continuing risk management cycle within each Federal agency, implement effective controls on information to address identified risks, promote awareness of information security risks among users, and act as a continual monitor and evaluator of policy and control effectiveness of information security practices.

In addition, the Federal Information Policy Act tightens the responsibilities of each Federal agency for implementing security procedures and policies that ensure the protection of its information systems. The CIO, in consultation with the Director of IN STEP, will have enforcement authority over individual agencies through his or her ability to make recommendations to the Director of OMB with respect to funding for information resources. This provision is necessary to ensuring that IN STEP can ensure accountability within each agency for information security management.

And finally, two other important features are included that are vital for the long-term development of flexible and responsive information security controls. The first is investing authority in the Director of IN STEP, through the CIO, to require Federal agencies to identify and classify the security risks associated with each of their information operations, and to calculate the risk and magnitude of harm that would result from an intrusion. IN STEP will have simultaneous authority to oversee the development and implementation of mandatory minimum control standards developed by NIST, that would be required for each classification. For this purpose, final authority is

given to the CIO, in consultation with the Secretary of Commerce, to decide and officially issue the standards. And the Act requires the Inspector General or an independent evaluator to conduct an independent evaluation of the information security program and practices of each agency on an annual basis, which will subsequently be reported to the U.S. CIO.

At the time when the growth and success of our competitive national economy is clearly demonstrating a correlation to the Information Revolution, the Federal Information Policy Act will secure the ability of our Federal Government to fully utilize information technology in order to better serve American citizens. And in a time when any entity-including government-that is connected to a computer needs to make information security a priority, we are finding that the Federal Government is dangerously behind the curve. We are losing time. FIPA will spur the actions needed to achieve readiness against future cyber security threats in a uniform and coordinated process. It is my hope that Congress will act on this measure as soon as possible so that the Federal Government will move forward and become a leader in the management and protection of governmental information systems.

VOLUNTEERS RESTORE ROSIE THE RIVETER'S VICTORY SHIP

HON. GEORGE MILLER
OF CALIFORNIA
IN THE HOUSE OF REPRESENTATIVES

Thursday, July 27, 2000

Mr. GEORGE MILLER of California. Mr. Speaker, earlier this month, the House of Representatives unanimously passed my legislation to create a Rosie the Riveter National Historic Park in Richmond, CA. H.R. 4063, which has been the subject of a hearing also in the Senate Energy Committee, would honor all those who served, in uniform and in coveralls, wearing helmets or bandanas, hoisting a machine gun or a welder's torch.

Rosie the Riveter is, in the words of the National Park Service, "the most remembered icon of the civilian work force that helped win World War II and has a powerful resonance in the women's movement." Rosie has been commemorated on posters, in the famous Normal Rockwell painting, and on a U.S. postage stamp. She remains one of the most enduring images of the Second World War.

Another icon does remain that is worth remembering and preserving is one of the 747 ships that the Rosies—and the Wendys and Welder—constructed at the Richmond Kaiser shipyards: the Red Oak Victory, one of the last surviving Victory ships that served in World War II. Eventually, the Red Oak Victory will play a crucial and permanent role in the National Historic Park. Today, she is being carefully restored by a small navy of volunteers that is stripping paint, cleaning rust, and reconstructing this legacy of the greatest war in history.

I want to pay tribute to the men and women who are volunteering their time to spruce up the Red Oak Victory so that future generations of residents, visitors and students can learn first hand about the home front efforts to win the war and the tremendous economic, demographic and social changes generated by the war effort.

The San Francisco Chronicle has published an account of the restoration effort, and I would like to share that report with my colleagues.

[From the San Francisco Chronicle, July 27, 2000]

ROSIE REVISITED—VOLUNTEER CREW IS RESTORING A WORLD WAR II VICTORY SHIP, REMNANT OF RICHMOND'S SHIPYARDS

(By Chip Johnson)

Every Tuesday for the past year, Owen Olson has left his Daly City home and stepped back in time aboard the Red Oak Victory, a World War II relic being brought back to life on the Richmond waterfront.

At 79 years old, the retired U.S. Navy lieutenant dons a pair of coveralls and safety glasses, and climbs down into the bowels of the ship's engine room to strip off layer upon layer of lead-based paint. His face streaked with oil, he is a Norman Rockwell image of an engine-room grease monkey.

Olson is one of the 30 volunteers, many of them retirees, who show up to paint, weld and repair the aging vessel. It is the only ship still afloat from Richmond's giant Kaiser Shipyards—a remnant of the glory days when 747 ships were built there during the war.

One day, they hope, the vessel will be docked at the Rosie the Riveter/World War II Home Front National Park in Richmond. The Rosie memorial, a 400-foot-long wall shaped like a section of a Victory ship, will tell the story of the working women—and men—of World War II. It is scheduled to be unveiled at a dedication ceremony in mid-October.

Meanwhile, about 7,000 feet of space at the old Ford plant, which built 60,000 tanks during the war, will be converted into a visitor center near where the Red Oak Victory would be docked in the future.

The visitor center will provide information about the shipyards, the tank factory and other World War II-era sites in Richmond as well as war-factory sites in Massachusetts, Washington, Michigan, Ohio, New York, Louisiana and Connecticut.

When the park is approved by Congress, it will become eligible for funding from the National Park Service. The visitor center is scheduled to be completed in two years.

Meanwhile, there is a lot of work to be done on the Red Oak Victory, whose restoration must be funded by grants and donations in addition to the sweat of volunteers who hope to have the job finished in two years.

On his weekly trip to Richmond, Olson is joined by a collection of aging wise guys and characters who look like they were typecast for a remake of "McHale's Navy," a 1960s TV sitcom.

The crew is clearly more comfortable aboard the ship—a rusting giant cargo vessel pulled from the mothball fleet at Suisun Bay two years ago—than they are on land. Some of the officers' quarters have been restored by a volunteer group from Clearlake in Lake County, but the rusting exterior decks and walls of the ship need the most attention.

Mike Huntsinger, a career merchant sailor, serves as the chief mate. His job is to coordinate the tasks on the ship and perform a mechanical assessment of the ship's condition. A detailed 60-page restoration report has just been submitted to a firm that will estimate the cost of repairing the 441-foot vessel.

"The objective is to restore it to an operating vessel and make it look like it did the day it was launched," he said.

Right now, the boat is docked in Brickyard Cove Marina at an old city-owned dock, Terminal 9. She is a rusting gray lady, but there are signs of life aboard her. A gigantic winch used to load one of the ship's four huge cargo holds has been restored and is now operational.

The 5mm and 20mm guns aboard the vessel, which was used to ferry supplies to soldiers fighting the Japanese, lie on the deck until the day they are mounted on the gun tubs on the bow and stern of the ship.

But making the Red Oak Victory whole again will take far more than the elbow grease and old sea stories that Olson and J.P. Irvin, his mate in the engine room, or chief engineer Bill Jackson can muster.

The cost is staggering—about $3 million to $4 million worth of mechanical repairs would require the giant vessel to be dry-docked. An equally long list of cosmetic work, including a stem-to-stern paint job, would also require a substantial investment, he said.

Sea valves in the ship's hull that once allowed ocean water inside to cool the engines have been welded shut. The propeller needs to be balanced, auxiliary generators could use an overhaul, and ultrasound tests must be performed on the hull, just to name a few things, Huntsinger said.

"We'll pare down from there and see what the real world gives us," he said.

Lois Boyle, president of the Richmond Museum of History, which owns the boat, will try to raise money through federal transportation grants, corporate sponsors—including Kaiser Permanente, whose parent company built the vessel—and hundreds of others.

The museum has also applied to have the ship placed on the National Register of Historic Places, which would qualify it for funding.

Despite its state of disrepair, the Red Oak Victory—named after the tiny town in Iowa that suffered the heaviest losses per capita in World War II—was a working merchant ship in the Vietnam War before being decommissioned in 1969.

Jackson, a veteran seaman who sailed for 53 years, knows the feeling. The 82-year-old Oakland native was living in Costa Rica with a new wife and new son when he got a call in 1990 from an old sea buddy to help run a steam-powered supply ship in Operation Desert Storm.

A few years later, Jackson returned to Oakland, where he lives with family members and spends his days aboard the Red Oak Victory.

"I love this ship and the sea and the friendships with the men that have sailed them over the years," he said.

He must love ships because during World War II, he had two of them torpedoed from underneath him. He survived, but suffered injuries aboard the Courageous, which was sunk off the coast of Trinidad.

The Red Oak Victory has become a rallying point for old sailors and history buffs alike, a place where they can work and reminisce and shave 30 years away.

Huntsinger remembers the feeling he had the first time he saw the ship.

"I saw the mast from the highway, came aboard and the memories came flooding back," he said.

As much as he and the rest enjoy the work, they will never turn away volunteers.

"I have a love for these old ships," said Rolly Hauck, 77 a retired salesman from Novato who served in the merchant fleet.

He and his compatriots have but one collective wish when it comes to the Red Oak Victory.

"I want to see this ship live again," Hauck said.