

CONGRESSWOMAN

ELLEN O. TAUSCHER

10TH DISTRICT ~ CALIFORNIA



1122 Longworth House Office Building – Washington, D.C. 20515 – (202) 225-1880 (phone) & (202) 225-5914
(fax)

FOR IMMEDIATE RELEASE
November 7, 2002

CONTACT: April Boyd (202) 225-1880
<http://www.house.gov/tauscher>

**Congresswoman Ellen Tauscher's Remarks To
Jane's Information Group's "Infrastructure Security Conference"**

<http://www.house.gov/tauscher/press/11-07-02.htm>

A year after the terrorist attacks against the United States, this forum offers a timely evaluation of what has been done to make our nation safer and what challenges remain. You have a number of great speakers who are getting into the details of the challenges facing specific sectors. Instead of giving you more facts and figures, I'd like to spend my time with you today sharing some observations that I hope will provide fodder for your discussions.

As a member of the House of Representatives, I have spent my Congressional career working to stop the proliferation of weapons of mass destruction. I have also been involved in the debate on homeland security for some time now, as one of the original members of Congress to advocate creating a cabinet-level Homeland Security Department, and I introduced legislation to that end with Senator Joe Lieberman and Congressman Mac Thornberry of Texas a year before the White House reluctantly embraced our idea.

I firmly believe that it doesn't make sense to have more than 40 government agencies responsible for counter-terrorism as we have today. My Wall Street business background and plain old common-sense tells me that by streamlining the bureaucracy to focus our counter-terrorism efforts, we can be more effective and use the additional leverage and clout to get the commitment and money it will take to succeed. If we are going to protect our national infrastructure, it's going to take a much better, more coordinated effort than we've had so far, and I believe that can only come from a streamlined bureaucracy focused under the umbrella of homeland security. If you look at the security of our seaports, airports, energy systems and cyberspace – I think it's clear that we are not as far down the path as we should be.

Port and Maritime Security

Rep. Ellen Tauscher

A number of observers have noted that the next likely threat to the United States will not be from a plane hitting a building or a nuclear reactor but from a ship carrying weapons of mass destruction hidden in a cargo container. The numbers are staggering. Some 11 million cargo containers worldwide are loaded and unloaded 10 times a day, yet there are no unified security standards governing how these containers are loaded and transported. More than 160 ships call at American ports every day – that translates to 60,000 ships delivering 6 million containers to the United States each year. The U.S. Customs Service screens data for all these containers, but physically inspects only about 2 percent of the volume of trade entering the country each year.

As security experts have noted, finding the right box to open, whether in the harbor of Los Angeles or Hong Kong, will depend mainly on good intelligence work to identify suspect shippers and questionable cargo. To put it bluntly, containers are a security nightmare. Because over half a million truckers, warehouse workers and freight handlers come into proximity with any given container, it's not a stretch to see how easy it would be for someone to slip a nuclear or bio-chemical device among the computer parts or apparel inside. An explosive device detonated in an American port would not only bring ocean commerce to a halt, but would cause all kinds of havoc. The impact would spread beyond the ports, to truckers and railroaders who move shipping containers to and from the docks, farmers who export perishable crops and retailers of everything from cars made in Asia to stores trying to get merchandise for Christmas sales.

As we saw with the recent West Coast port lockout a few months ago, a shutdown can cost the U.S. economy as much as a billion dollars a day. Although port vulnerability studies will not be completed for another five years, there are steps that can be taken to improve security in the short term.

Lawrence Livermore National Laboratory, for example, is developing better cargo inspection devices that will enable Customs to inspect more containers in less time, thereby reducing disruption to the flow of commerce. But out of an estimated need for some \$2 billion to harden security at seaports, only \$92 million has been authorized and approved by Congress. More work must be done in this area.

And finally, trade security should be approached as a layered process with inspections of containers at receiving ports being the last step in the process. The Bush administration's Container Security Initiative, which requires major foreign ports to verify the security and contents of containers before they are loaded onto ships bound for the United States, is an important way of ensuring that weapons of mass destruction are not smuggled into our country. It is particularly important that we have gotten Hong Kong – a port that ships six thousand containers to the United States every day – to sign on to this program. We've seen problems arise with the way the Bush administration has gone about getting some of the European countries to sign on to this program, but I believe in the end these diplomatic glitches that have become so common for this administration will get worked out and the shipping program will move forward.

Between the time cargo is loaded at a foreign port and inspected in the United States, we need effective tracking systems to ensure that the contents of the cargo containers are not altered

during the crossing. The Transportation Department is preparing Operation Safe Commerce, a \$28 million demonstration project to improve maritime cargo security by tracking shipments from overseas. If we can get a number of private companies to participate by letting their overseas cargoes be used as a test bed for improved security, we will effectively be able to push the secure perimeter way beyond the United States to the foreign ports where the containers are loaded.

Regional cooperation is crucial, and I welcome the recent signing of STAR, the Secure Trade in the Asia-Pacific Economic Cooperation Region, which calls for member countries to screen both goods and people before they are transported, increase security on ships while en route and tighten security at seaports.

Aviation Security

While securing our ports is a major piece of the puzzle, most people, understandably, focus on securing our skies because of the way our country was attacked on September 11. Since many of you flew to be here today, I don't have to tell you about how important air travel is. But airlines are no longer just an important part of our transportation infrastructure. Air travel has become a major part of how the world does business and how the American and global economies function.

America's aviation industry is a national asset, and Congress has to act responsibly to ensure that it doesn't become the public's biggest fear and our economy's biggest threat. We've been doing that by taking airlines out of the security business and making screeners federal employees with vigorous background checks, uniform training and standards. We are also strengthening cockpit doors, and we established the Transportation Security Administration to ensure the FAA can focus on its core mission, which is flight safety.

But I am concerned that the approach that has been taken so far has been about airport security and not aviation security.

While the Transportation Security Administration is working to deploy a nationwide federal screening workforce by November 19, I am concerned that other equally critical security measures are being overlooked. The sweeping aviation security legislation passed a year ago mandated background checks for all employees with access to secure areas at the airport, including caterers and maintenance personnel. But I am concerned we are stopping way short of the goal.

Little to no improvement has been made to secure the perimeters around tarmacs or to require that anyone with access to a plane have a tamper-proof identification card with high-tech biometric identifiers. Without these measures, there's no way to be sure the guy driving the Coke truck up to the airplane is really Harry the Coke truck driver. We also haven't done enough to address the gaping holes at flight schools and private airports.

In addition to security challenges, I believe it would be prudent to examine some of the law's unintended consequences. Capital construction costs are soaring because the floors and walls of

many airports cannot even support the new explosive screening machines the law mandates, and several airports are struggling with the citizenship requirement for screeners, especially airports in large metropolitan areas like my home outside of San Francisco.

Energy Systems

But where aviation security has become a matter for the federal government to solve, the federal government cannot hope to step in and provide security for each and every installation in our country's vast energy infrastructure. Because 85 percent of America's infrastructure is controlled by the private sector, securing it is one of the hardest challenges before us. Instead, the federal government will have to harness the capabilities of the private sector to achieve a prudent level of security without hindering economic growth, productivity or trade.

First, the new Department of Homeland Security, if we ever get one, in partnership with the private sector, needs to build a comprehensive database of vulnerabilities and preparedness of critical targets across the nation's infrastructure. As you know, there are a number of barriers to improved information sharing between the private sector and the government, mostly because companies have concerns about liability on one side and the government's inability to discuss classified information on the other. This is a difficult problem, but one approach that has merit is enacting an "Omnibus Anti Red Tape" bill. The law would provide, among other things, a fast-track security clearance process that permits the sharing of secret level classified information with appropriate non-federal and industry leaders. This law could be one of the first items to be discussed by the legal panel described in the White House's Homeland Security Strategy. The panel, convened by the Attorney General with representatives of state Attorneys General, state legislators, state law enforcement, the FBI, the EPA, Health and Human Services and other relevant agencies will meet to propose needed legislative reform or guidance on statutes governing public disclosure.

The second issue related to risk assessment and information sharing is terrorism insurance. In addition to the homeland security agency legislation and our remaining appropriations bills, I hope that terrorism insurance will be one of the bills we address in the lame duck session next week. The federal government needs to work with states to enhance market capacity to cover terrorist risk so that companies can continue to expand and the United States remains an attractive place to do business.

Of the various components of our energy supply, civilian nuclear power plants are what many people worry about. The Nuclear Regulatory Commission has taken a number of steps to improve security and plants are now protected by armed guards, massive structures and multiple backup systems.

Among the recent recommendations by former Senators Gary Hart and Warren Rudman to ensure the safety of the energy grid is a stockpile of modular backup components to quickly restore operation of the grid should it fail. Lawrence Livermore National Laboratory has a program to do just that, producing proliferation-proof modular nuclear reactors that can be used to provide energy for isolated rural communities.

Cyber Security

Like securing our energy infrastructure, cyber security is also a complex challenge. Cyber security is unique, though, in that it cuts across a number of responsibilities, sectors and legal issues – spanning law enforcement, national security, civil rights, and commercial and private sector interests. Cyber information is most often a private good, with 80 percent of all information systems owned by the private sector, making it hard to legislate boundaries, codes of conduct or access to information.

The December 2001 Gilmore panel on the defense of physical infrastructure states that the convergence of video, satellite and telephone communications; the Internet; and other day-to-day conveniences like ATM machines will increase the risk of a carefully engineered cyber attack disrupting multiple networks and systems.

I am concerned that the issue of computer security has become even more urgent in recent months. You might remember a few weeks ago when one of the largest and most sophisticated assaults in the history of the Internet crippled 9 of the 13 computers that manage global Internet traffic. The attack was defeated, but the President's top cyber security advisor, Dick Clarke, has warned about our vulnerability to future attacks because many public and private computers have not been successfully configured to block outsiders. Although it's a crime to enter a computer without authorization, the CERT Coordination Center at Carnegie Mellon University, which acts as a clearinghouse for information about intrusions, viruses and computer crimes, reported that the number of incidents rose from 406 in 1991 to nearly 53,000 last year.

The Gilmore Panel makes a number of recommendations, of which I would reiterate two:

First, since 80 percent of information systems are owned by the private sector, any new directives or solutions need to be arrived at through partnership and cooperation with private entities.

And, we should always be re-examining our vulnerabilities. We should look at the panel's recommendation that the President establish an entity to develop and implement a comprehensive plan for research and development, testing and evaluation to enhance cyber security.

At a time when our physical and cyber infrastructures are increasingly interconnected and interdependent, bringing these two authorities under the same roof makes sense. Indeed, the devices that control our physical systems – including our transportation systems, distribution systems, dams and other infrastructure – are increasingly connected to the Internet.

War on Terrorism

Even with a large increase in funding for homeland security, the creation of a new homeland security agency at some point in the future, and seamless information sharing between the government and private sector about vulnerabilities and corrective measures, all our efforts are doomed to fail if we do not keep pursuing the War on Terrorism. It makes little sense to spend

millions on improving the security of the power grid if we are not equally committed to disrupting al Qaeda's networks abroad.

The United States can and must do better to disrupt terrorist financing.

An October report by a commission sponsored by the Council on Foreign Relations says that America's "efforts to curtail the financing of terrorism are impeded not only by a lack of institutional capacity abroad, but by a lack of political will among U.S. allies. . . . Confronted with this lack of political will, the current administration appears to have made a policy decision not to use the full power of U.S. influence to pressure or compel other governments to combat terrorist financing more effectively."

This, along with a Defense Department seemingly spread too thin, causes me great concern.

I question how the administration can contemplate a ground war in Iraq and still fulfill important commitments elsewhere such as Kosovo, Bosnia, the Philippines, and Afghanistan – where we still don't have a "Marshall Plan" and we haven't secure one square foot outside of Kabul. Despite a successful military operation in Afghanistan, security remains tenuous, an Afghan Army has yet to be fielded, and food aid and reconstruction efforts are insufficient. At a time when we are engaged in a global War on Terrorism, it is critical that the administration explains how our finite resources are going to be used. Those plans must honestly assess all the unfinished tasks and challenges in the fight against al Qaeda.

What should we focus on?

In addition to recommitting ourselves to the War on Terrorism, I believe the administration needs to do a better job sorting through the threats facing our nation and prioritizing them in order of credibility and imminence – not only for the sanity of the American people, but also to maximize our ability do something to protect ourselves.

Since the terrorist attacks, Americans' understanding of asymmetric threats – the kind of unpredictable attacks intended to cause chaos and disrupt our lives and economy – has grown. The television news channels regularly discuss nightmare scenarios involving dirty bombs, widespread outbreaks of small pox, or today's report of bubonic plague in New York. Recent public reports indicate that the intelligence community has caught foreign terrorists talking admiringly about the sniper who recently paralyzed the D.C. area, which, understandably, has raised concern that Islamic extremists will soon put snipers in other American cities.

While the public's understanding of asymmetric threats has gotten more sophisticated, counter-intuitively, Washington's response has not.

Just a few weeks ago on October 22, the White House asked American oil, gas and transportation industries to beef up security by strengthening physical barriers and improving surveillance. Yet, according to the administration, there was no specific threat.

And you thought your job was tough – imagine a chemical plant owner or water treatment manager who is told by the White House to worry about snipers, planes falling out of the sky, truck bombs and cruise missile, anthrax and chem-bio attacks. While I want to be careful not to discount the seriousness of each of these threats, I have to question whether publicly raising a number of different threats in such a vague way is helpful or harmful for overall preparedness and performance.

One of the objectives of the National Strategy for Homeland Security is to implement a homeland security advisory system that characterizes appropriate levels of vigilance, preparedness and readiness in a series of graduated threat conditions with corresponding action to be taken in response. You know this as Tom Ridge's color-coded warning system. You also probably know it as the punch line of many late-night talk show jokes. It's understandable why.

On September 24 of this year Attorney General John Ashcroft and Governor Ridge downgraded the threat level from high – or orange – to elevated – or yellow. They said this was "based on a review of intelligence and an assessment of threats by the intelligence community."

Three weeks later, on October 17, while the threat was still at its lower yellow level, CIA Director George Tenet testified before Congress that – to quote, "The threat environment we find ourselves in today is just as bad as it was last summer [meaning prior to September 11]. They [meaning Al Qaeda] are reconstituted. They are coming after us. They are planning in multi-theaters. They are planning to strike the homeland again."

Despite Director Tenet's warning, Governor Ridge kept the threat level at yellow. No wonder people are confused, given the two totally different messages coming from high-ranking Bush administration officials. This isn't part of some sub rosa conversation. Incongruent messages are coming from the mass media which broadcast the press conference about Governor Ridge's latest color code change and then aired Director Tenet's dire warning without even noticing the serious discrepancy between the two.

I know that Governor Ridge has announced that the administration is putting together a comprehensive list of potential targets that if struck would cause the greatest disruption to the United States. Maybe he should come talk to you guys.

Tough fiscal choices

As I mentioned earlier, I supported a bill to establish a Homeland Security Department months before the administration thought it was a good idea, in fact, when the White House was fighting it tooth and nail. And over the last year, I have voted for a number of bills to protect everything from airports and shipping to our energy supply and food resources.

If our nation wants to be able to better protect the critical infrastructure that makes the United States the most modern and wealthiest economy on the planet, it's time to do what's really hard and make some tough fiscal decisions in Washington.

In a article that ran in late September on public opinion about the war in Iraq, the *Washington Post* carried a picture of a demonstrator in New York City whose sign read "Our Grief is Not a Cry for War." What this woman meant was that her pain and that of others who lost their loved ones on September 11 should not be used to endorse the President's use of force against Iraq.

The White House has used September 11 and its aftermath to justify a lot of spending and policy decisions, including a possible war in Iraq and increased funding for National Missile Defense. At a time when we are dripping in red ink, we need to choose between policies and programs that are designed to help the American people and those that have little connection to the real threats to our national security. The American people don't have endless wallets, our economy is tapped out and the White House can't keep putting everything that's tangentially related to homeland security into the category of high risk.

The economy is growing, but so is our budget deficit. I am concerned that we are reaching an unsustainable situation. The administration, which claims to be fiscally conservative, insists on spending billions for National Missile Defense, which has little or no relation to the current terrorist threats we face.

Compounding this, a recent survey of city officials by the Public Policy Institute of California reported that many city officials believe that their local residents would not support higher taxes to increase terrorism readiness. Despite a near tripling of homeland security funds for fiscal year 2002 – to 70 billion dollars – the Institute notes that "city officials are asking for state and federal funding to train emergency response personnel, purchase emergency equipment, and pay for threat prevention and detection efforts." And, the U.S. Conference of Mayors is reporting that 79 percent of mayors have a funding shortfall for necessary threat detection equipment; 77 percent need emergency response equipment and 69 percent have first-responders without the necessary protective apparel.

So, given this difficult fiscal picture, where is the administration looking for savings? "Little boutique programs in the education budget," according to Office of Management and Budget Director Mitch Daniels.

Instead of trying to nickel and dime our way to a balanced budget with small but vital public education programs, I think the more responsible thing to do would be to objectively examine how we are spending our national security dollars. Some of the funding currently going to expensive, less immediate programs like a National Missile Defense shield might be put toward better use securing our homeland against what everyone acknowledges is our most significant threat – terrorism.

I understand the White House's frustration that members of Congress and administration officials continue to request big funding increases for their own pet projects. However, their conclusion that the way to avoid the guns-or-butter mistake is to question everything that's not security related and advocate without question everything that is, seems to be wrong-headed.

States and municipalities ahead of Washington

Rep. Ellen Tauscher

It is clear that success in making our nation safer will ultimately reside in simultaneous progress made at the local, state and federal levels. Frankly, Washington should get poor marks for its failure to streamline the current bureaucracy into a new Department of Homeland Security. And the White House took eleven months to produce a National Strategy for Homeland Security that critics, including myself, think isn't as much a strategy as it is a recitation of excuses we've heard before to justify military action we already know they want to take.

States and local governments are doing surprisingly well – in spite of the absence of a strong national strategy or a department – because they have already started coming up with their own solutions to basic vulnerabilities. Local governments in Kansas and Missouri are planning, sharing assets, and responding to emergencies through an existing body called the mid-America Regional Council that was originally formed to deal with fires and agricultural emergencies. Pennsylvania has perfected a system called the Pennsylvania Justice Network – or J-Net – which acts as a conduit connecting previously incompatible databases. J-Net gives a law enforcement officer seated in her squad car access to a one-stop-shop on her computer that allows her to check for electronically scanned fingerprints, criminal histories, drivers license photos and lists of inmates and parolees. Unfortunately, information from the INS is not included, but I think this is a good start none-the-less.

In another example of smart thinking, first responders and law enforcement officers in Arlington, Virginia, have solved the issue of incompatible communications systems so that all relevant groups can be alerted at once – unlike the situation in New York when police received orders to evacuate the World Trade Center towers but firefighters using different radios did not. Today, in the back room of the Alexandria Police Department's dispatch center, there is an equipment rack holding over a dozen different radios, from a dozen different agencies, from Metro to the D.C. Fire Department to the U.S. Park Police. They are all wired together so that when a signal comes through one of the radios, it is immediately translated and sent back through the other departments' radios to the entire system. It took the Pentagon attack for that to happen. I don't think we should be responding to attacks – we need to be preparing for them.

In the area of California that I represent, the Contra Costa Water District, with little or no federal directives, has already taken a number of steps to review and strengthen the security of its water system. But there are a lot of vulnerabilities in any water system – like water treatment plants, an open canal, several reservoirs and hundreds of miles of pipes. Like local agencies across the country, the Contra Costa Water District needs more money from somewhere – most likely the federal government – to deal with the numerous vulnerabilities they face.

As is true for other states, California has taken a number of steps to address potential vulnerabilities and prepare for a possible attack based on its experiences. Lessons learned about interagency command and control from our experience dealing with earthquakes and fires have provided local authorities with a foundation on which to build their response to potential terrorist attacks.

As a recent RAND study put it, "all types of terrorist attack tactics have been seen in California. . . in past attacks or are currently residing or travelling through the state." However, while officials in California are generally well prepared for health emergencies, fires, earthquakes and floods,

like in other states across the country, more work needs to be done in terms of information sharing and performing risk assessments if we are to improve security.

Conclusion

So where are we – really?

Despite a tripling of the homeland security budget for fiscal year 2002, I noted that states and municipalities are still asking for more funds to improve their homeland security preparedness. One of the reasons why homeland security needs are not going away is that much of the money appropriated by Congress was provided to help recover from the terrorist attacks, for victim relief and to improve security at various sites around the country – in other words, immediate, one-time expenditures.

The latest Hart-Rudman report describes this as a reactive approach to improving homeland security, and it should concern all of us. In their new report, former Senators Hart and Rudman, now co-chairmen of the Council on Foreign Relations task force on homeland security, warn that the "federal government is dedicating an extraordinary amount of energy and resources in response to the specific character of the September 11 attacks." Indeed, after the terrorist attacks, we rushed to pass the \$2 billion Aviation and Transportation Security Act of 2001 which focused the Transportation Security Administration almost exclusively on hiring federal employee screeners and deploying massive explosive-detection machines to check luggage. This reaction made sense since we had all just witnessed hijacked commercial airliners being rammed into buildings. But Hart and Rudman warn that "a reactive mindset is inevitably wasteful in terms of resources and can distract agencies from anticipating more probable future scenarios and undertaking protective measures."

As we work to decrease and defend against our infrastructure's vulnerabilities, I believe it is important that we not simply fight the last war, but also concentrate on doing a better job of identifying real and future threats to our homeland.

And finally, I believe that the way we address the challenge of terrorism will do much to define our society. In the end, our society should still be open and globally engaged – not paralyzed by fear or, as some have said, "trapped behind the modern version of moats and castles."

###