KOSTAS
Research Institute
for Homeland Security

"The New Homeland Security Imperative: The Case for Building Greater Societal and Infrastructure Resilience"

Written Testimony
prepared for a hearing of the

Committee on Homeland Security and Governmental Affairs
U.S. Senate

on

"The Future of Homeland Security: Evolving and Emerging Threats"

by

Stephen E. Flynn, Ph.D.
Founding Co-Director
George J. Kostas Research Institute for Homeland Security &
Professor of Political Science
Northeastern University
s.flynn@neu.edu

Dirksen Senate Office Building - Room 342
Washington, DC

10:00 a.m.
Jul 11, 2012

"The New Homeland Security Imperative:
The Case for Building Greater Societal and Infrastructure Resilience"

by

Stephen E. Flynn, Ph.D.
Professor & Founding Co-Director, Kostas Research Institute
Northeastern University

Chairman Lieberman, Ranking Member Collins, distinguished members of the Committee on Homeland Security and Government Affairs, thank you for the opportunity to testify before you as a part of this important series of hearings on the future of homeland security. Mr. Chairman, I first testified on this topic on October 12, 2001, when you held the gavel of the predecessor of this committee, the Committee on Governmental Affairs. That was just one-month after the tragic attacks of September 11, 2001. At that time, I concluded my testimony by observing: "Terrorists have declared war on this homeland. This nation is extremely vulnerable to these kinds of attacks. We need to come to grip with that fact and recognize that we have to fundamentally rethink and reorganize how we provide for the security of this nation in this new and dangerous era." Thanks to the leadership provided by this Committee and especially both you, Mr. Chairman, and Senator Collins, considerable progress has been made towards repairing what was essentially a broken system for managing the kind of threat posed by al Qaeda more than a decade ago. I want to personally express my deepest respect and gratitude for the extraordinary service you have provided this nation. But the threat continues to evolve, and the challenge of securing the American homeland is an extremely complex one. Accordingly, it could not be more timely and appropriate to take stock at this juncture of where we are and where we need to go to advance the homeland security mission.

Assessing the Threat:

As my fellow witnesses can speak to in more detail than I, the state of the al Qaeda threat in 2012 is a good news and not-so-good news story. The good news is that the successful dismantling of so much of al Qaeda's senior leadership infrastructure including the May 1, 2011 death of Osama bin Laden, has reduced the capacity for al Qaeda to plan and execute sophisticated large-scale attacks on North America. The not-so-good news is that there is a continued risk of small-scale attacks executed by homegrown and other affiliated terrorists of al Qaeda and that these attacks are more difficult to prevent. Major attacks require a group of operatives directed by a leader, communications with those overseeing the planning, and time to conduct surveillance and rehearse the attack. Money, identity documents, safehouses for operatives, and other logistical needs have to be supported. All this effort ends up creating multiple opportunities for detection and interception by intelligence and law enforcement officials. Alternatively, small attacks carried out by 1-3 operatives, particularly if they reside in the United States, can be carried out with little planning and on relatively short notice. As such, they are unlikely to attract the attention of the national intelligence community and the attacks, once underway, are almost impossible for the federal law enforcement community to stop.

While the move towards carrying out smaller-scale attacks undoubtedly reflects a practical necessity of a much diminished core al Qaeda, these attacks also reflect a growing realization that terrorist attacks on the United States do not have to be spectacular or catastrophic to be effective. As the attempted bombing of Northwest Airlines Flight Number 253 on Christmas Day 2009 dramatically illustrated, even near-miss attacks can generate considerable political fallout and a rush to impose expensive and economically disruptive new protective measures. Since relatively small and unsophisticated attacks have the potential to generate such a big-bang for a relatively small investment, the bar can be lowered for recruiting terrorist operatives, including those who belong to the targeted societies.

The October 2010 air cargo incident involving explosives hidden ink cartridges shipped from Yemen is consistent with this trend towards smaller attacks, but with the added element of aspiring to create significant economic disruption. The would-be bombers had no way of knowing that the cartridges would end up on a commercial airliner with hundreds of passengers or a dedicated air cargo carrier with a small crew. That was not important since they understood that destroying any plane in midair would trigger U.S. officials and others to undertake an extremely costly and profoundly disruptive response that would undermine the movement of global air cargo.

Beyond the threat posed by al Qaeda, there is a more worrisome reality that arises from the otherwise enviable position associated with the United States standing as the world's sole superpower. Quite simply, it has become reckless for our current and future adversaries to challenge the United States by engaging in the kind of warfare we are best prepared to fight. Their better option is to take the battle to the civil and economic space as opposed to engaging in direct combat with our second-to-none armed forces. Targeting innocent civilians and critical infrastructure such as the intermodal transportation system, mass transit, refineries, food supply, and the electric power grid holds out the best promise for producing mass disruption to essential systems and networks, and in generating widespread fear. As such, even if al Qaeda disappeared tomorrow, acts of terrorism and cyber attacks will be the asymmetric weapons of choice for state and non-state actors intent on confronting U.S. power in the 21st Century. We need to improve our capacity to defend against those attacks by reducing our vulnerabilities and building greater resilience so as to assure the continuity or rapid restoration of critical functions, services, and values in the face of disruptive events.

The Limits of Going on the Offense

In response to the attacks on 9/11, the Bush Administration mobilized U.S. national security capabilities to go after al Qaeda and those within the international community who supported them. To an overwhelming extent, the strategy was one of prevention by way of military force supported by stepped-up intelligence. On May 19, 2004, Vice President Dick Cheney summarized the effort this way: "Wars are not won on the defensive. To fully and finally remove this danger (of terrorism), we have only one option—and that's to take the fight to the enemy." The hoped for outcome of engaging the threat in Iraq and Afghanistan and around the world, President George W. Bush declared on July 4, 2004, was "so we do not have to face them here at home." This

strategy has involved a considerable amount of national treasure. According to the Congressional Research Service, between 2001 and 2011, Congress approved $1.28 trillion dollars for the Operation Enduring Freedom (OEF) Afghanistan and other counter terror operations; Operation Noble Eagle (ONE) providing enhanced security at military bases; and Operation Iraqi Freedom (OIF).[1] That amount translates into a burn-rate of $350 million for each and every day for ten years. By contrast, the cost of one-hour of these war operations—$15 million—has been the most that has been invested in the entire annual budget for the Citizens Corps Program which was initiated after 9/11 to engage citizens in the homeland security mission by volunteering to support emergency responders.

While a case can be made that going on the offensive in the global war on terrorism has paid off in preventing another catastrophic terrorist attack on U.S. soil, as the testimony of this panel today makes clear, the danger of terrorism has not been removed. Instead it has changed, while other evolving threats to the homeland continue to grow.

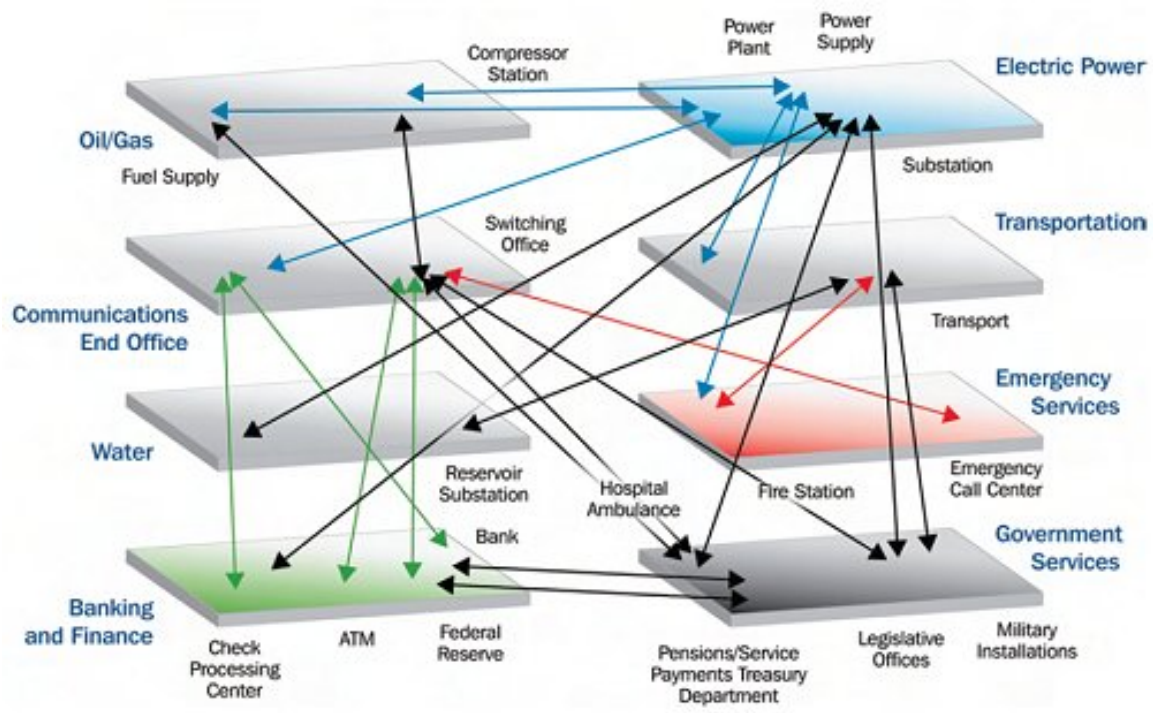
The Growing Cyber Threat:

The cyber security threat is clearly one of the most serious economic and national security challenges we face as a nation. Quite simply, the United States is at risk of becoming a victim of its own success. Our position as the world's dominant economic power can be attributed in no small part to the speed at which Americans have developed and embraced information technology systems and applications. But while we have been leading and benefiting from the information age, there has been too little consideration to the security implications of our growing reliance on information technologies.

A particularly worrisome vulnerability is the extent to which over the past decade, more and more Internet Protocol (IP) devices have been replacing legacy hardware, software, and communications protocols for the nation's physical infrastructure. As industrial control systems (ICS) become increasingly accessible to the Internet, cyber attacks can be launched at the electrical power grid; water and waste management systems; oil pipelines, refineries, and power-generation plants; and transportation systems ranging from mass-transit to maritime port operations. An attack on these systems by a state or non-state actor, not only places at risk the security of sensitive data and the disruption of essential services, but the potential for catastrophic loss of life and destruction of property. This is because computer hackers are not only able to infiltrate systems, but they are increasingly in a position to actually take control of such systems – turning off alarms or sending bad data that falsely triggers an alarm. Unfortunately, these cyber attacks need not be terribly sophisticated in order to accomplish substantial harm. Because of the interconnectivity of our networks, successful disabling of just one critical system can generate cascading consequences across multiple systems.

[1] Amy Belasco, The Cost Iraq, Afghanistan, and Other Global War on Terror Operations Since 9/11. Congressional Research Service, Mar 29, 2011, http://www.fas.org/sgp/crs/natsec/RL33110.pd.

POTENTIAL CASCADING EFFECTS OF ELECTRIC POWER FAILURE



Source: Department of Homeland Security[2]

The ongoing vulnerability of transportation systems to mass disruption:

Mass transit systems and rail freight are likely to become increasingly attractive targets for terrorist organization. These systems are relatively easy to access since they provide multiple entry points, very often over a vast geographic area, with little to no physical security barriers to entry. Homegrown terrorists are likely to be familiar with these systems. Attacks on mass transit, especially stations, particularly when undertaken during peak-commuting hours, can potentially be even more deadly than an attack on a single aircraft. At the same time, should such an attack lead to the shutting down of a transit system, the resultant denial of service can be crippling to the operation of a major urban economy.

The intermodal transportation system also remains extremely vulnerable to mass disruption. Despite new security initiatives advanced in the aftermath of 9/11, there

[2] National Aeronautics and Space Administration. NASA Science News. Severe Space Weather – Social and Economic Impacts. June 2009 at http://science.nasa.gov/science-news/science-at-nasa/2009/21jan_severespaceweather/

remains too few meaningful measures in place for detecting and intercepting a determined terrorist that is intent on placing a shielded nuclear device in a container with the goal of generating fear that leads to the slowing or stopping of the flow of cargo containers into U.S. ports or across our land borders. Particularly worrisome is that virtually all containers that Customs and Border Protection currently targets as suspicious enough to warrant an inspection, are not actually examined until after those containers arrive at a U.S. port which are often in major urban areas where other critical infrastructure is concentrated. This remains the situation despite the fact that CBP currently has inspectors in 58 overseas ports as a result of the Container Security Initiative that was begun in 2002 for the stated purpose of facilitating collaboration with foreign customs officials so that targeted containers would be inspected before they are shipped to the U.S. ports.

On February 6, 2012, CBP Acting Assistant Commissioner Kevin McAleenan testified before the House Subcommittee of Border and Maritime Security that the total amount of containers inspected overseas in 2011 was just 45,500. This represents 0.5% of the 9.5 million manifests that CBP stated that the agency reviewed overseas in advance of loading. If the 45,500 number is divided by the 58 CSI ports and 365 days per year, the result is CSI inspectors are examining with their foreign counterparts on average, 2.15 containers per day per overseas port before they are loaded on carriers bound for the US--two containers each day.[3] This does not represent much of a deterrent. As the ongoing incidence of contraband smuggling, trade fraud, and cargo theft make clear, we have a long way to go in securing global supply chains against the threat of proliferation as well as the nightmare scenario of transportation conveyances being used as a WMD delivery device.

Natural Disasters as the clearest and most present homeland security danger

In addition to the ongoing risk associated with terrorism, there is an even more clear and present danger to the safety of Americans that should animate the homeland security mission: natural disasters. One need look no further than the news headlines from the past 2-3 weeks for confirmation of this reality: severe storms and power outages across the mid-Atlantic states, wildfires in Colorado and Utah, and devastating floods in Minnesota and Wisconsin. It turns out that 91 percent of Americans live in places at a moderate risk of earthquakes, volcanoes, tornadoes, wildfires, hurricanes, flooding, high-wind damage according to an estimate calculated for *Time* by the Hazards and Vulnerability Research Institute at the University of South Carolina.[4] This translates into virtually all of us being on tap to experience several major disasters in the course of our individual lifetimes. Then too, there is the risk of major pandemics and the occasional large industrial disasters such as the Deepwater Horizon oil spill and the nuclear

[3] "Balancing Maritime Security and Trade Facilitation: Protecting Our Ports, Increasing Commerce and Security the Supply Chain." Joint Testimony of David Heyman, Paul Sukunft, and Kevin McAleenan before the House Committee on Homeland Security, Feb 7, 2012: 10.

[4] Amanda Ripley, "Floods, Tornadoes, Hurricanes, Wildfires, Earthquakes … Why We Don't Prepare, TIME, Aug 20, 2006.

meltdown at Fukushima Daiichi Nuclear Power Plant. The bottom-line is that our safety requires greater levels of preparedness to deal with risk at home.

Recalibrating the Homeland Security Enterprise

Coping with the array of threats and vulnerabilities that remain more than a decade after 9/11 requires a recalibrated approach that places new emphasis on localized, open, and inclusive engagement of civil society. Recently, it has been the actions of ordinary citizens that have been critical to thwarting terrorism threats on U.S. soil. In the case of the attempted car-bombing on New York's Time Square in May 2010, it was a sidewalk T-shirt vendor, not a nearby police patrol officer who sounded the alarm about Faisal Shazhad's SUV. On Christmas Day 2009, it was courageous passengers and flight-crew members, not a federal air marshal, that disrupted the suicide-bombing attempt by Umar Farouk Abdulmutallab aboard Northwest Airlines Flight 253.

Everyday civilians, supported by state and local officials, will need to be better informed and empowered to play a meaningful role. This role includes not only preventing acts of terrorism, but making investments that mitigate the risk of disruption to our communities and critical infrastructure. This will require a homeland security enterprise centered around three efforts: (1) setting appropriate expectations, (2) increasing transparency, and (3) building community and infrastructure resilience.

Setting Appropriate Expectations. Elected officials with the support of national security professionals need to avoid promising more than the federal government can reasonably deliver. As a stepping-off point, leaders of both political parties should publicly acknowledge that there are inherent limits to what can be done to prevent acts of terror. No security regime is foolproof. Risk is a fact of life and making decisions about how best to manage those risks involves difficult tradeoffs. When new technologies and security protocols are deployed, they should not be oversold. Creating unrealistic expectations guarantees public anger, disappointment, and mistrust when a terrorist attack succeeds. The goal should be for a security regime to be able to survive a "morning-after-test;" that is; it should be able to withstand a postmortem where the public concludes that the regime consisted of reasonable safeguards, even if they were not infallible. The goal should be to have adaptive security systems that adjust based on an ongoing assessment of threat, vulnerability, and consequence.

Increasing transparency. U.S. national security and federal law enforcement agencies need to resist the secrecy reflex. On the surface, it seems sensible to tightly control information about vulnerabilities or security measures that potential adversaries might exploit. But these restrictions can undermine the defense of critical infrastructure, such as seaports, dams, and waterworks. In determining the best way to protect a suspension bridge, for example, the bridge's chief engineer is likely to have ideas that would not occur to a law enforcement or national security professional. But strict rules that preclude the sharing of homeland security information with unvetted individuals too often translates into leaving essential expertise on the sidelines. Even when security information is shared with vetted company security officers, they are precluded from passing along the details to their bosses who do not hold active security clearances. As a

result, investment and operational decisions are often made with scant attention paid to the potential security stakes.

The federal government should make a concerted effort to increase transparency with the broader public as well. Many policymakers believe that candor about potential dangers may generate excessive public anxiety. However, people are most frightened when they sense not only their vulnerability to threats, but feel powerless to address them. U.S. officials have stated for nearly a decade that terrorism is a clear and present danger, but they have given citizens little information about how to cope with that hazard. Instead, citizens are told to proceed with their daily routines because their government is hard at work protecting them. The psychological effect of this is similar to that of a doctor telling a patient that she is afflicted with a potentially life-threatening illness and then providing only vague guidance about how to combat it. No one wants to receive disturbing news from his physician, but a prognosis becomes less stressful when doctors provide patients with all the details, a clear description of the available treatments, and the opportunity to make decisions that allow the patient to assert some personal control over the outcome. In the same way the federal government can decrease the fears of terrorism by giving the American public the information it needs to better withstand, rapidly recover, and adapt to the next major terrorist attack.

Building Resilience:

Terrorist attacks perpetrated by homegrown operatives who act along or with one or two-accomplices are more difficult to detect and intercept. As a result there is a greater probability that these less-sophisticated attacks will be successful. At the same time, the resultant damage from a small-scale attack is likely to be localized and far less than typically experienced during and after a natural disaster that Americans have become largely accustomed to coping with. Therefore, the incentive for launching small-scale attacks on U.S. soil lies with causing our society to react in a way that amplifies the direct damage generated by the attack. In other words, how we respond to acts of terrorism effects our adversaries' calculation about undertaking these attacks. If we provide them with a "big bang" for their relatively modest, buck, we end up fueling the incentive for terrorist activity. Alternatively, if the result was something of a fizzle, there will be little to be gained from carrying out these attacks.

As a way forward, Washington should place greater emphasis on developing adequate societal and infrastructure resilience. Resilience is the capacity of individuals, communities, companies, and the government to withstand, respond to, recover from, and adapt to disruptive events. Since disruptions can come not just from terrorism but also from natural and accidental sources as well, advancing resilience translates into building a general level of preparedness.

Ideally, a program of resilience would address the most likely risks that people, cities, or enterprises may face. This would minimize the potential for complacency while assuring a level of basic skills, such as first aid and effective emergency communications, which are useful no matter the hazard.

A program of resilience requires individuals, communities, and companies to take precautions within their respective areas of control. Success is measured by the continuity or rapid restoration of important systems, infrastructure, and societal values in the face of an attack or other danger.

Resilience begins on the level of individuals. A program of resilience would promote self-reliance in the face of unexpected events, encouraging civilians to remain calm when the normal rhythms of life get interrupted. It would also teach individuals to make themselves aware of the risks that may confront them and to be resourceful by learning how to react to crises. And it would make preparedness a civic virtue by instructing civilians to refrain from requesting professional assistance unless absolutely necessary, thus freeing up manpower for those in the greatest need.

Promoting individual resilience involves acknowledging that many Americans have become increasingly complacent and helpless in the face of large-scale danger. Reversing this trend demands a special emphasis on educating young people. Students should learn to embrace preparedness as both a practical necessity and an opportunity to serve others. These students, in turn, can teach their parents information-age survival skills, such as texting, which may offer the only means to communicate when cellular networks are overloaded (800 text messages consume the same bandwidth as a one-minute call). As demonstrated in the aftermath of the 2010 Haitian earthquake and the Deepwater Horizon oil spill that same year, social media are transforming the way rescuers and survivors respond to crises. These new tools have the power to turn traditional, top-down emergency management on its head.

Resilience also applies to communities. The U.S. government can promote resilience on the communal level by providing meaningful incentives for collaboration across the public, private, and nonprofit sectors before, during, and after disasters. Much like at the individual level of resilience, communities should aspire to cope with disasters without outside assistance to the greatest degree possible.

Building resilient communities requires providing community leaders with tools to measure and improve their preparedness based on a widely accepted standard. The Community and Regional Resilience Institute, a government-funded research program formerly based at Tennessee's Oak Ridge National Laboratory and now located at the non-profit Meridian Institute, has spearheaded an attempt to define the parameters of resilience, modeled on the method by which fire and building codes were created and are maintained. Led by Warren Edwards, it has drawn on a steering committee that I was privileged to chair and a network of former governors and former and current mayors, emergency planners, and academics to develop detailed guidelines and comprehensive supporting resources that will allow communities to devise resilience plans tailored to their needs. Other countries, including Australia, Israel, and the United Kingdom, have instituted similar programs. Federal and state governments could provide communities that implement a comprehensive risk-awareness strategy and a broad-based engagement program with tangible financial rewards, such a reduced insurance premiums and improved bond ratings.

U.S. companies compose the third tier of resilience. Resilient companies should make business continuity a top priority in the face of a disaster. They should invest in contingency planning and employee training that allow them to serve and protect their customers under any circumstance. Corporations must also study the capabilities of and partner with their suppliers and surrounding communities. Much like individuals and communities, corporations with resilience would possess the ability to sustain essential functions and quickly resume their operations at full capacity after a disaster. Resilience may also bring financial benefits to companies able to demonstrate their dependability in the wake of a major disruption. Such companies are likely to experience an increase in market share by maintaining regular customers and attracting new ones as well.

Although most large corporations invest in measures that improve resilience, smaller companies—which are the backbone of local economies and yet are constrained by limited resources—generally do not. But small businesses can rectify this in a low-cost manner by creating a buddy system between companies located in different regions. For instance, a furniture store in Gulfport, Mississippi, that may fall victim to an August hurricane could partner with a furniture store in Nashville, Tennessee, that may suffer from spring flooding. These businesses would agree to assist each other in providing backup support for data, personnel, customers, and suppliers in the event of a disaster.

To his credit, President Obama has explicitly identified resilience as a national security imperative in his May 2010 National Security Strategy. Homeland Security Secretary Janet Napolitano did the same in the February 2010 Quadrennial Homeland Security Review. Both have made frequent references to the importance of resilience in their speeches. But much more needs to be done to tangibly advance this agenda, and it will require an all-hands approach. This is why I along with my colleague Peter Boynton feel so privileged to have been appointed the founding co-directors of the George J. Kostas Research Institute for Homeland Security at Northeastern University.

I have long argued that universities and colleges have been a largely overlooked national resource in advancing the homeland security enterprise. Beyond the academic Centers of Excellence established by the Department of Homeland Security, and courses and programs designed to educate homeland security professionals, the higher education community has largely sat on the sidelines as federal, state, and local governments have struggled to find their way in the post-9/11 world. This not the case at Northeastern where President Joseph Aoun has made security one of three areas of strategic emphasis for its growing research enterprise. In addition, thanks to the generous gift of Northeastern alumnus and trustee, George J. Kostas, the university has built a new facility that offers a secure environment for innovative translational research conducted by private-public-academic multidisciplinary research teams.

At the Kostas Institute, our mission is to help advance resilience in the face of 21st Century risks. We have made community resilience and infrastructure and systems resilience our primary area of focus. We are a particularly interested in identifying and advancing ways to "bake-in" to the operations and design of critical systems, especially those involving transportation and information, so as to enhance their security, integrity, and continuity in the face of man-made and naturally occurring disasters. Given the

historic leadership role that Northeastern, our neighboring universities, and the information technology industry that is concentrated in the metro-Boston area have played, we feel a special responsibility to help manage the growing risks to critical systems from cyber threats. To this end, we are committed to bringing together expert researchers and practitioners to identify risks and their potential consequences, to develop next-generation secure applications and computing architecture, and to promote best practices with our counterparts around the U.S. and globally.

Conclusion

For most of the 20th Century, the United States was able to manage our national security as the equivalent to an away game; that is; by confronting threats beyond our shores. That all changed on September 11, 2001. Yet as a nation, we continue to struggle with defining the appropriate role and investment that the federal government should make in managing our ongoing vulnerability to terrorism and other catastrophic risks on U.S. soil. From the standpoint of resources, the investment Washington makes in homeland security remains a fraction of the resources devoted to traditional national security. At times, this can have the perverse outcome of actually making civilian targets potentially more attractive to our adversaries. For instance, the U.S. Navy has invested more in protecting the single port of San Diego that is home to the Pacific Fleet, than the Department of Homeland Security has invested in the ports of Los Angeles, Long Beach, San Francisco, Oakland, Seattle, and Tacoma *combined* upon which the bulk of the U.S. economy relies.

It will take determined leadership to recalibrate our national and homeland security efforts to better managed the evolving and emerging threats that confront us. Mr. Chairman, throughout your long and distinguished career in the U.S. Senate, you have been providing that leadership. I commend you for the instrumental role you have played in advancing the safety and wellbeing of this great nation.

I want to thank you for the opportunity to once again testify before this committee today. I would be happy to answer any questions you may have.