THE GEORGE WASHINGTON UNIVERSITY
HOMELAND SECURITY POLICY INSTITUTE

STATEMENT

OF

FRANK J. CILLUFFO
DIRECTOR
HOMELAND SECURITY POLICY INSTITUTE
THE GEORGE WASHINGTON UNIVERSITY

BEFORE

THE U.S. HOUSE OF REPRESENTATIVES

COMMITTEE ON HOMELAND SECURITY
SUBCOMMITTEE ON ECONOMIC SECURITY, INFRASTRUCTURE PROTECTION AND CYBERSECURITY

"PREVENTING TERRORIST ATTACKS ON AMERICA'S CHEMICAL PLANTS"

JUNE 15, 2005

Chairman Cox, Chairman Lungren, Ranking Member Thompson, Ranking Member Sanchez, and distinguished members of the Committee, it is a privilege to appear before you today. The House Committee on Homeland Security should be commended for continually reassessing and reevaluating our efforts to secure the nation's critical infrastructure, including today's issue, the chemical industry.

Recognizing the important roles that the private sector and the government play, the Committee has assembled a cross-section of the chemical industry as well as the Department of Homeland Security. This is important because Congress must understand both perspectives to receive a complete picture of accomplishments, and areas for improvement, since 9/11. My specific focus will be on the significance of a public-private partnership for homeland security policy. To this end, I will delineate how we can establish the "business case for homeland security" across the chemical industry and beyond. Each witness will have his own insights and recommendations regarding the threat and potential solutions, but we must not take our eye off the ball and allow our individual interests to obstruct the overall mission.

We are all meeting today with the common purpose of better protecting citizens by ensuring that the nation is doing all it can to bolster security. But we have a few questions to answer. As a key component of the nation's critical infrastructure, what are this sector's roles and responsibilities? What are the federal government's responsibilities? What do we measure and are we measuring the right things? And, how much is enough? My hope is that the solutions discussed during today's hearing can serve as a foundation for future legislation and strategy as we continue to refine our tactics to fight the war on terrorism. We must also not limit ourselves by looking at the chemical industry in isolation—as many of the issues we face in this sector are relevant to protecting critical infrastructure writ large. Homeland security requires a multifaceted strategy to prevent, protect against and respond to 21st century threats. We need to develop further guidelines to help us build upon the significant progress we have made thus far in securing our nation's chemical sector, but we must consider all aspects of a solution—constantly developing new approaches to the problem. We cannot rely solely on yesterday's weapons and strategies to fight tomorrow's battles and defeating a dynamic network of enemies will require our own dynamic network of domestic and international allies that will include all levels of government, the private sector, communities and individuals.

Terrorists turned commercial planes into missiles on 9/11, swiftly and viciously awakening the nation to the challenges before us today. It was eminently clear that the war on terrorism would not be anything like the wars of the previous century and the new enemy shares little in common with the previous one. Al Qaeda and its ilk do not exhibit traditional characteristics or fall under any conventional military definitions, representing an asymmetrical, constantly morphing threat that is symbolic of the challenges we now face. Terrorists targeted the symbols of the nation's public and private sectors on September 11, as they struck both the World Trade Center and Pentagon, negating the traditional, centuries-old security barrier of two large oceans. We now face an enemy consisting of a network of affiliated groups who span national borders and jurisdictions and use non-traditional weapons in battle without distinguishing between soldiers and civilians. We do not face an adversary that we can defeat in a conventional war on a traditional battlefield by going plane for plane or tank for tank, but one that will take the path of least resistance by constantly searching for our greatest vulnerabilities. They have declared war on every American and threaten all segments of the U.S. economy and with that, the global economy. Bin Laden has repeatedly said he intends to "[bleed] America to the point of bankruptcy." Recognizing the enemy's strategy, we must embolden the industries that underpin our nation's economy. We now fight a war that requires us to play both offense and defense, pursuing the terrorists abroad and keeping them on the run, while also bolstering our defense at home. Experts agree that an attack on the nation's chemical sector, which includes more than 15,000 facilities engaged in the production, use, storage and distribution of toxic products, could have potentially catastrophic consequences.

Against this background, we must understand that this is not a war that can be solely fought and won in Washington but needs the innovation, hard work and input from individuals across all sectors of the economy. It is more than just guards, guns and gates. The thousands of private sector companies that own and operate the energy, banking, finance, agriculture, telecommunications and chemical sectors, among others, underpin the American economy, and all have a significant role to play in our strategy. Given the interdependency of all of the sectors, a unanimous commitment will be essential. The war on terrorism is the calling of our generation and we must adapt our existing organizations, structures and processes to meet the new threat. Innovation, rather than the status quo should be emphasized since the terrorists are not static and base their actions on our actions. And because of the constantly evolving threat, we must always strive to stay ahead of the curve. The bureaucratic

structures and strategies of the past will not adequately meet the challenges of the future, and a new organizational paradigm is vital to confront emerging threats and enemies. We must marshal and mobilize all of the available expertise and latest technology in the private and public sectors as we devise and execute a comprehensive strategy to win the war. But we also cannot make the mistake of looking for new solutions through our rearview mirror. Rather, we need to view homeland security through a prism, considering every perspective and how each company, industry or department fits within the overall mission. We do not want to be in a position where we are constantly reacting to their actions—as the adversary adapts, finding our next greatest weakness. Thus it is necessary to address all potential threats in a proactive manner.

We want to reduce the risks and mitigate the consequences of an attack on our chemical sector and ensure that we are not merely shifting risks and creating new, unforeseen risks. We must prioritize, using a risk management-based approach that looks at homeland security holistically, and execute a strategy based on an equation of vulnerabilities, threats and consequences. The approach can be applied to all levels of government and the private sector as we define and redefine our priorities in the years to come.

Recognizing that the private sector owns and operates more than 85 percent of nation's critical infrastructure, a public-private partnership for chemical security is both sensible and necessary. The government's control over the production, use, transport and distribution of at-risk chemicals is limited and comprehensive security requires the concerted investment and support of the private sector. The National Strategy for Homeland Security notes that "a close partnership between the government and private sector is essential to ensuring that existing vulnerabilities to terrorism in our critical infrastructure are identified and eliminated as quickly as possible." Further, the National Strategy for Physical Protection of Critical Infrastructures and Key Assets, calls for this to be a "shared responsibility." I could not agree more with this sentiment and fervently believe we need to look at the entire supply chain as we refine our strategy.

The government has made tremendous strides since 9/11 in securing our critical infrastructure. Key players in the chemical industry have also made significant advances to upgrade security—meeting both business and national interests. What we now need is for government and industry to work together to develop a playbook that

they can use to drive planning and preparedness. A comprehensive assessment of where the industry is in terms of security accomplishments needs to be completed as we draw a roadmap for the future. This cannot and should not be a one-size-fits-all approach, but instead should be catered to the unique strengths and weaknesses of each industry.

When addressing homeland security issues and the public-private relationship, conventional Washington wisdom is to search for an easy solution, often turning to regulation and mandating industry to comply with new federal requirements. But homeland security requires a more novel, nuanced approach if we are to succeed—one that will obligate the government to veer from the standard practice of pronouncing new "though shalts." Regulations often hamstring growth and innovation, and lead to added expenses without taking industries' costs, concerns and previous measures into account—simply, they do not provide a practical or comprehensive solution. We cannot just place requirements that make us feel good; instead we must ensure what we do matters. A December 2004 report on cybersecurity issued by this committee's Subcommittee on Cybersecurity, Science, and Research & Development, concluded that "it is important to realize that industry may be incentivized to do more than government could regulate." I agree and contend that this conclusion is appropriate for the chemical industry as well. Regulations can create a "check the box" mentality, where industry does just enough to meet the requirements and are disinclined from making proactive homeland security investments.

We need the experts driving security, not the trial lawyers. I have found that industry is generally willing to participate in security initiatives and adopt the government's goals and mission if they are viewed as a partner in the policymaking process. It is up to government to engage the business community and articulate why such initiatives are mutually beneficial to both the public and private sectors. The government needs to set the bar and raise it high through leading by example and getting its own house in order. It can help drive best practices and standards that can then be overseen by DHS and/or a trusted third party. The private sector should be asked to take security as far as it can, but since industry will not always be able to reach the bar on its own, the government must work with the private sector to help it meet the goals it set. The government and the insurance industry can provide incentives/aid to industry to help meet those standards.

We all understand that security and safety are tightly interwoven in the post-9/11 world and we need to look at chemical industry security using an all-hazards approach. We do not need "satisficing," which only leads to an industry vying for the lowest common denominator. So as we build upon recent private and public sector initiatives, how can the government make a compelling business case for homeland security that satisfies all parties and most importantly, betters the security of our citizens?

The Business Case for Homeland Security

In an April 2005 speech to business leaders at the U.S. Chamber of Commerce, Secretary of Homeland Security Michael Chertoff appropriately stated:

"We want to defend our country, but we also want to defend our way of life…Our goal is to create a security environment that works with the grain of commerce and doesn't cut against it, and that takes advantage of and leverages with the great American ingenuity, which is our principal weapon."

The government is eminently well-suited to lead in some areas while the private sector has its own unique strengths. What we must do is marry-up private sector interests with public responsibility. The solution will require a private-public partnership that looks at the entire supply chain and approaches security using a risk management model. We need to reduce risk while mitigating the consequences of an attack. A successful business case for homeland security should include the following:

- Public-private information sharing and delineation of roles
- Analysis and assessment of threats, risks and vulnerabilities
- Identification of the secondary, tertiary benefits of security
- Highlighting of best practices, standards
- Oversight by government and/or trusted third party
- Carefully designed metrics that ensure progress
- Rewards and incentives for security
- Regulations, as a last resort

Cultivating public-private coordination and information sharing—We must begin by fostering a trusted partnership between the federal government and the chemical industry based on cross-sector communication and information sharing. We need to refine the game plan based on a more symbiotic relationship which ensures

significant and timely security progress. The federal government has significant expertise and the best information on the adversary (including intentions, capabilities and modus operandi) that the chemical industry will need to successfully implement its roles and responsibilities. And the chemical industry owns the infrastructure the government is endeavoring to secure. The government can provide the framework and the industry, as the experts in their field, develop voluntary standards. All information, whether time-sensitive threat information, best practices or vulnerability assessments, should be part of a trusted information sharing effort. The government must properly communicate the threat the industry faces, keeping the sector informed of the latest intelligence, realizing that this changes with time and is often difficult to predict.

Information should flow both ways, from top-down and bottom-up. At Fedex, for example, the company readily shares information with the government because the company's leaders feel they have a duty to protect the homeland. As Fedex CEO Fred Smith said to his peers in Chief Executive magazine: "By taking responsibility for shoring up points of vulnerability in the physical and Cyberspace worlds, companies can truly defeat those who would harm our way of business and our way of life. I urge all businesses to become partners with government in making our companies, our country and, ultimately, our world more secure." Since action is stronger than words, I point to Fedex's participation on the FBI's Joint Terrorism Task Force (JTTF), the only such company in the nation to have such a role.

Those corporations that have developed best practices should then be encouraged to share these with the federal government as well as their colleagues in the industry. The government needs to ensure that the Freedom of Information Act (FOIA) exemptions and antitrust provisions passed in the 2002 Homeland Security Act remain and are strengthened to ensure continued information exchange. The development of the Homeland Security Information Network (HSIN), which serves as a real-time, two-way information clearinghouse for both DHS and industry is another important initiative. Other existing programs are in need of a reevaluation, however. One such program is the Protected Critical Infrastructure Information (PCII) Program, which lacks the protections, much less the incentives, that industry desires.

In promulgating Homeland Security Presidential Directive 7 (HSPD-7), President Bush clarified the need for cross-sector planning, information sharing, risk assessment and coordination. The president directed each federal department to engage its

stakeholders as partners for the purpose of strengthening the security of our key industries. The Risk Analysis and Management for Critical Asset Protection (RAMCAP) initiative is a prime example of how cross-sector cooperation can make major headway in analyzing threats and vulnerabilities and sharing information. A cooperative DHS-chemical sector project begun late last year, RAMCAP will eventually lead to a more systematic analysis of terrorist threats on the nation's chemical sector and other infrastructure using a risk-based approach. Aspects of the project include the development of a Security Vulnerability Analysis (SVA) methodology that will provide each sector with the tools and metrics for the analysis of threats as well as supplementing the National Asset Database (NADB) with industry-specific information and screening tools. In short, it will help us define our greatest vulnerabilities, delineate the threat, and highlight best practices for the industry.

The chemical industry has a seat at the federal government's homeland security table with last June's formation of the Chemical Sector Council, overseen by 16 associations representing the spectrum of the chemical industry. Sector Coordinating Councils are intended to bring together the critical infrastructure protection stakeholders from key industries together with federal, state and local agencies. The Chemical Sector Council identifies, prioritizes, and coordinates the protection of the chemical industry's infrastructure and facilitates information sharing for threats, vulnerabilities, incidents and best practices. Now that the industry groups are together, DHS should immediately develop a framework with these groups and identify mutually agreed upon incentives and timelines that would accomplish what all sides want: a better protected and prepared chemical industry. Such a partnership would provide a better investment of public and private dollars than regulations alone. The essential point is that each side should see that it has something to gain by contributing. The coordinating council also provides a mechanism for government-to-industry communication that will enable one to build upon the other's previous work and ensure that each side's roles and expectations are properly communicated. What we cannot afford is a "double sunken cost," where the private sector takes the initiative to invest on its own in homeland security, only to have it superseded by regulations requiring another cost.

Developing standards and metrics— As I previously noted, the government needs to raise the bar and keep it high, ensuring that the standards by which the industry are judged are as clear as possible. Standards should be initiated by the private sector and

overseen by Uncle Sam and/or a trusted third party. Members of the American Chemistry Council (ACC) follow a self-initiated Responsible Care Management System, which requires companies to assess vulnerabilities and develop action plans, but the ACC includes less than 10 percent of at-risk facilities and the care code lacks fixed metrics and standards for quality control. Industry-wide, definable standards are needed to ensure the more than 15,000 facilities currently regulated by the EPA are secure from terrorist attacks. Such standards and expectations must be clear for all actors across the supply chain from producers to transporters to distributors. For example, the government cannot reasonably expect the chemical industry to provide air defense for their facilities, a public good that few would argue is the responsibility of the private sector.

Standards must meet security requirements and ensure due care without bankrupting industry or the federal government. The government could then indemnify those organizations that meet the standard from all actions above and beyond their capabilities, hence the government assumes the role as the insurer of last resort, as is the case for conventional warfare. In developing its own "Good Housekeeping Seal of Approval," the federal government would create an industry-wide objective that every chemical production, transportation and distribution facility would endeavor to fulfill. It is not inconceivable that citizens, looking to invest in socially responsible companies meeting a government-approved standard, ask the federal government for a list of those organizations taking security seriously. Thus the standard could provide a financial benefit to industry, with the market, not the government driving security. Among similarly priced goods, the security seal of approval could be the difference among consumers.

We must have metrics to measure the needs of the chemical industry as well as its accomplishments. As the adage goes, "what gets measured, gets done." However, we must ensure that what we are measuring actually matters and that it is actually paying security dividends. There must be a time component in the metrics as well, given that there is an imperative for action almost four years after 9/11. What we are measuring and the actions taken as a result must be a balanced approach for a given industry, company, or geography, given the dynamic risk, threat, and vulnerability environments.

The standards developed should be overseen by the government and/or trusted third party. Currently, chemical plant security is primarily overseen by the EPA and DHS.

The EPA regulates the 15,000 Risk Management Plan (RMP) facilities under the auspices of the Clean Air Act, but DHS now has lead responsibility for securing the nation's critical infrastructure. Protecting critical infrastructure is a security and emergency management priority and no longer strictly an environmental issue. We need to take a comprehensive view and defend against both intentional and accidental chemical incidents, requiring us to look at chemical plant security with the all-hazards approach to safety and security. Moving full authority for the development and oversight of standards of chemical facilities to DHS would provide the chemical industry with a single authority on security matters. Given the DHS mission and the new reality, the department is particularly well positioned to provide leadership in this area.

Identifying the secondary benefits to security—Like the successful efforts to improve quality in the 1980s and safety in the 1990s we must embed security as part of businesses' missions by helping industry see the secondary benefits of security. Just as the Ford Motor Corporation adopted the mission that "Quality is job one" in the 1980s, in a post-9/11 world, security should be job one for the chemical industry. Industry discovered collateral benefits of quality assurance and safety, and it is incumbent upon the federal government to stress the manifold benefits of security for national interests and each organization's bottom line. The government must emphasize the importance of business continuity and that addressing security issues will help companies preserve market share and maintain operations during both manmade/terrorism-related and natural disturbances. Organizational resiliency and the effort to standardize processes across the entire supply chain will have long term benefits for business as they seek to cope with everything from terrorist attacks to supply shortages to worker strikes.

The role of Chief Security Officers and Chief Information Officers need to be strengthened within the organization. CSOs and CIOs should not be viewed as cost centers, but instead as integral components of the leadership team that position security as a benefit rather than an expense. This is an issue for the boardroom, not the backroom or the boiler room. Security and profits are not mutually exclusive concepts and there are clear economic benefits for investments in security. Investments in security are often considered against investing in other profitable parts of the organization. But it is clear that new revenue, new businesses, new products and other secondary benefits can be found through security spending. Companies can get a return on investment (ROI) in security and a number of companies are heeding

the national call for homeland security—seeing the potential for security, as well as financial dividends.

Asset visibility and tracking, standards development, collaboration within the supply chain and physical and personnel security can do a lot to secure the nation as well as improve organizational efficiency. For example, utilizing GPS systems and RFID tags to monitor chemical goods will enable industry to more predictably and accurately track the flow of products, find exceptions in the system and track security breaches—all economically significant improvements linked to improving security. Security upgrades such as digital video monitoring systems in chemical facilities can also assist in emergency incident management and theft reduction. The secondary benefits to background checks on personnel, reinforcing plant physical security and improving communication among supply chain parties all have obvious security and economic benefits and are avenues for the government and private sector to pursue mutual interests. A dollar spent on homeland security could mean a dollar saved—providing a double bang for the counter-terrorism buck. This concept is transferable to all infrastructure sectors.

Leaders in the chemical industry should be applauded for their self-initiated efforts to secure the homeland. Since 9/11, over $2 billion has been spent by ACC members alone. The 140-plus ACC member companies operating more than 2,040 facilities have enacted laudable, self-imposed security standards. Representing 90 percent of the nation's chemical production, the ACC has moved the ball down the field, but we are still too close to our own goal line. Despite their significant spending, ACC members only represent 7 percent of the nation's at-risk chemical facilities, and pending assessments, it is unclear how much has been accomplished industry-wide.

Companies outside of the chemical industry have made security a priority. At FedEx, more than 500 law enforcement officers now place terrorism at the top of their list of priorities—along with traditional needs like theft prevention. Implied here is that the company sees secondary and tertiary benefits of security, among them improved product control, tracking and overall efficiency. But individual attempts by the private sector can only go so far, just as government-initiated programs have limited utility. Coordination is crucial and a symbiotic relationship between the government and private sector is required to get us to the next level.

We need to develop and implement dual-use technology that shows the clear economic incentives of security. Recent government/shipping industry initiatives

exemplify a viable business case for security. More than 9,000 importers and other shipping organizations have realized that they can increase efficiency, productivity and profits through security by engaging in the Customs-Trade Partnership Against Terrorism (C-TPAT) program. The program requires companies to bolster security by protecting their supply chains from terrorists in exchange for quicker processing and fewer inspections. The government gets the security and assurances it is looking for and the private sector gets greater efficiency and revenue. The National Strategy for Homeland Security notes that benefits of security to industry are self evident, making the "internalization of…costs…not only a matter of sound corporate governance and good corporate citizenship but also an essential safeguard of economic assets for shareholders, employees, and the Nation." To this end, the government needs to initiate policies that do more than stress the merits of "good corporate citizenship," and instead incentivize the chemical industry to secure the nation's hazardous chemicals by communicating the numerous benefits of security. Policy without resources is just rhetoric and the government needs to appeal to industry as good businessmen and good citizens. Society stands to benefit, not just in homeland security terms, but from the secondary environmental, health, safety and anti-crime benefits as well. The private sector could take much credit for these accomplishments, if the business case is adopted.

Establishing incentives—As I previously testified at a July 2001 hearing before the Joint Economic Committee, only "through leading by example can the government realistically hope for the private sector to commit the sort of effort—in time and resources—expected of them." I stand by this statement and continue to advocate a paradigm where the government leads by example, getting its own house in order by setting standards and developing best practices. It can then provide incentives to the private sector to make security a priority, while avoiding regulation that could stifle the growth and the natural market flow. On any CEO's wish list of outcomes from a proactive security strategy are lower insurance premiums, reduced legal liability, reduced tax liability, safe-harbor provisions, recognition from the government and its private sector peers, enhanced reputation, and reduced incident response and recovery costs.

Some of these wishes can already be fulfilled through proper utilization of the SAFETY Act, a potentially powerful liability elimination tool for sellers and customers of anti-terror products and services. The SAFETY Act is particularly relevant for the chemical sector, as it provides an incentive to facility owners to

invest in their own security. Facility owners purchasing SAFETY Act certified technologies or services increase their security (by simple virtue of purchasing security tools) and decrease their liability exposure. A facility owner knows that it is purchasing a valid, effective product thanks to the rigorous evaluation process the seller must undergo before any SAFETY Act award is granted by DHS. And, of course, the owner will also receive immunity from lawsuits. DHS can assist in encouraging the use of the SAFETY Act by granting its benefits to more technologies and services – and that is something Secretary Chertoff has repeatedly committed to doing.

We should consider having the federal government serve as the insurer of last resort, by assuming a burden above and beyond what the private sector and the insurance industry is able to bear. The government may also need to consider anti-trust exceptions that will encourage information sharing between competitors. These are not unreasonable and I believe can be accomplished if we build a solid business case for homeland security.

It is important to point out that it is not just about money, but also information. The previously cited December 2004 subcommittee report on cybersecurity also lists a number of the aforementioned incentives as ways the government can leverage the private sector in promoting security. These incentives equally applicable to the chemical sector, as they are to cybersecurity. And as the report states, legislative mandates cannot be "both a floor and a ceiling" since in a free market, regulation could lead to an unprofitable (and thus untenable) situation.

The private sector too has a responsibility to develop incentives. The insurance industry in particular has tools at its disposal that could effectively incentivize critical infrastructure owners and operators. Just as the insurance industry drove municipalities toward stricter building codes and a focus on fire prevention, rather than only responding to fires, so too could the insurance industry incentivize the chemical industry to take proactive action. The insurance industry already has a complex matrix of discounts to encourage good behavior of various kinds, from non-smoking to ergonomic shop floors. And though developing insurance models for terrorism is difficult (and some would say, impossible), it is possible to recognize that some proactive actions not only reduce losses from a terrorist attack, but also provide important safety and anti-crime benefits as well. This expected reduction in insurance claims should be passed along to the private sector in the form of lower premiums,

which will in turn encourage other companies to take proactive, dual-benefit security measures.

Recognizing performance—For those corporations that meet the industry-set standards, the federal government should publicly commend the corporations' accomplishments, provide government incentives and encourage private sector incentives. The DHS Homeland Security Advisory Council and the Council on Competitiveness should be commended for their calls for a homeland security award for private industry akin to the prestigious Malcolm Baldrige National Quality Award. A parallel effort should be fostered by the private sector. For the chemical industry, a major national organization would seem to be well positioned to recognize the accomplishments of its own.

Enact regulations, if necessary—If, and only if, the market is unwilling or unable to meet the bar, increased DHS oversight and regulations should be carefully considered. However, we must realize that regulating the chemical industry could quickly become a slippery slope for other sectors as well. This could lead to a situation where, for example, the information and telecommunications sector becomes regulated as a knee jerk reaction. Given the constantly evolving threat, we must not turn to a one-size-fits-all approach and create regulations that could lose utility with the next intelligence estimate.

If regulations are enacted, the costs, both to the government as well as the chemical industry, must be considered. The costs for implementing regulations will be significant to both parties. For example, legislation proposed in the last Congress that would have provided DHS with regulatory oversight of the chemical industry was estimated to cost the federal government more than $200 million over the first five years. And the chemical industry must understand that regulations do not necessarily mean that the government will assume all costs. Thus it is always my contention that we should mitigate before regulate or litigate and a successful business case can and should forestall most federal regulations.

Conclusion

The chemical industry is the focus of this hearing, but the strategies we discuss today can be translated to the dozen other critical infrastructure sectors. Security is not merely a challenge, it is an opportunity for us to put our heads together and surpass our own assumptions. The task is enormous, and it requires efforts on every front. We

must learn from our successes, as well as our mistakes and refine our efforts accordingly. We cannot shy from this task because of its magnitude. We can and must overcome it. Spending alone, whether private or government dollars, will not thwart terrorist attacks to critical infrastructure. It takes the collective actions and commitment of the government and the private sector to secure the facilities that we all can agree are critical to our nation. Above all, we cannot afford for our slow action to lead the public to lose trust in our ability to secure the nation. That's at the heart of today's hearing.

As I conclude, I would like to congratulate Chairman Cox on his recent nomination to head the Securities and Exchange Commission. Your leadership on homeland security issues and commitment to making this committee a permanent, standing body (no easy feat) is widely respected and appreciated. The SEC will be in good hands upon your confirmation. And I will add that you will be in a unique position to look at the business case for homeland security in your new capacity. Chairman Lungren, Ranking Member Sanchez, Ranking Member Thompson, your leadership and vision on the issues is also to be applauded, and I look forward to continuing to work with all of you and your colleagues on this issue and other matters that arise in the future. Mr. Chairman this concludes my statement. I would be happy to answer any questions you may have.