As Prepared for Delivery

The Honorable Tom Ridge
President and CEO of Ridge Global
First Secretary, U.S. Department of Homeland Security

Senate Homeland Security and Governmental Affairs Committee
September 11, 2013

The Department of Homeland Security At 10 Years:
Examining Challenges and Achievements and Addressing Emerging Threats

Good morning, to my former House colleague, Chairman Carper. To Ranking Member Coburn, thank you for the invitation. To distinguished members of the Homeland Security and Governmental Affairs Committee, thank you for the opportunity to be with you today.

I am Tom Ridge, President and CEO of Ridge Global. Prior to heading Ridge Global, and following the tragic events of September 11th, I became the first Assistant to the President for Homeland Security. In 2003, I was honored to become the first Secretary of the U.S. Department of Homeland Security (DHS), where I had the privilege to work with more than 180,000-plus dedicated employees of the department.

I am testifying today in my personal capacity. However, I also chair the U.S. Chamber of Commerce's National Security Task Force. The task force is responsible for the development and implementation of the Chamber's homeland and national security policies and is a voice for businesses across America—both large and small. This position certainly informs my perspective on many issues.

I welcome the opportunity to appear here to examine ways in which we can secure America's future. I recognize that we have limited time here, so I request the opportunity to revise and extend my remarks for the record.

Before I begin I want to, on this anniversary, acknowledge the families that lost loved ones on September 11, 2001. We all love our country. The reason we are here is to work together to do our best to ensure that such events do not happen again and that other families do not have to suffer like those of our 9/11 heroes.

I was invited here today to provide my views on *The Department of Homeland Security At 10 Years: Examining Challenges and Achievements and Addressing Emerging Threats*.

With your indulgence, I would like to make two general observations first, and then focus on what I believe is a cross-cutting issue that both DHS and the broader federal government have faced in the past-- and it has the potential to complicate our future.

It is becoming clear that members of this body intend to pass some form of immigration reform. DHS components can be expected to play a significant role in implementing these reforms. My position is that the time has come to grant status to those who wish to enter to our

country legally, to work lawfully, and to pay taxes. But unless the Congress balances this approach by providing for effective enforcement mechanisms and providing adequate resources to the men and women of Customs and Border Protection, ICE and Border Patrol, and Citizenship and Immigration Services (CIS), DHS will be unable to meet its mission, regardless of the political plan you put in place. We can talk about reaching consensus in Washington, but unless reforms are resourced, DHS components will be saddled with an impossible mission in the critical area of border security.

On a related note, I have been concerned about the number of critical senior-level vacancies at DHS. In particular, as Congress debates immigration reform and with tensions high in the Middle East, DHS has had no permanent Secretary, no confirmed Deputy Secretary or General Counsel. And vacancies remain for Director of Immigration and Customs Enforcement and Under Secretary for Intelligence and Analysis. While several key nominations were recently made, several of these positions were open for months. Earlier this summer, as many as 15 senior positions were unfilled. This comment is not directed at Acting Secretary Beers or other dedicated public servants who, in their acting capacities, are doing their best under the circumstances. Such a high number of DHS vacancies should be disconcerting at any time. I urge the Administration to fill remaining vacancies quickly and the Senate to, in a judicious but timely manner, exercise its advice and consent responsibilities.

Mr. Chairman and members of the Committee, considering your topic today: *The Department of Homeland Security at 10 Years: Examining Challenges and Achievements and Addressing Emerging Threats*, I would like to spend the rest of my time discussing the challenges of information sharing. This issue has been with us since 9/11 and cuts across a range of challenges that have and will continue to confront the dedicated men and women of the Department of Homeland Security and their partners.

The nature of the terrorist threat has changed. As we have seen in Iraq, Afghanistan and today in Syria, our enemy is no longer just Al Qaeda, but like-minded organizations and nation-states that are willing to ally themselves in order to harm their common enemy—the United States. In my opinion, this will require the intelligence community to renew its commitment to work more closely with one another than ever before. Congress, in its oversight role, should ensure that DHS specifically remains plugged into the federal intelligence community horizontal. For if intelligence indicates a physical or cyber threat against the homeland, DHS will be required to work with our partners along the vertical—with state and local governments and critical private sector owner-operators—to address the concern. Further, we should ensure that the great progress that has been made for information sharing with state and local partners—such as the establishment of fusion centers—continues to be nurtured.

No discussion of the DHS threat environment or about information sharing can be complete without discussing cyber security in more detail. There is no part of our national economy, infrastructure, or social fabric that is not in some way connected to the internet backbone. Our critical power and communications, transportation and product supply chains, and financial systems. And DHS owns many of these sector-specific relationships.

This cyber threat is not new or emerging. In fact, when I was Secretary, in 2003, a full decade ago, the first US *National Strategy to Secure Cyberspace* was released. Greater awareness of this threat may be emerging, but the threat itself has been with us and will be with us for the rest of our lives.

As the first Secretary of Homeland Security, I believe I have perspective on this issue. We learned after 9/11 that information sharing and coordination at all levels of government—and with the private sector—would be critical to preventing future attacks and being resilient if attacks did occur. This was acknowledged in the development of the initial *National Strategy for Homeland Security*, the *National Infrastructure Protection Plan* as well as numerous other strategic documents and subsequent revisions overseen by Secretaries Chertoff and Napolitano.

After Hurricane Katrina, in post-disaster report after post-disaster report, we learned that the private sector brought great capabilities to the response and that improving collaboration between the public and private sectors would be critical in future emergencies and necessary to make our country more resilient.

Now, today, threats in the cyber world are getting quite a bit of attention. I have heard many of my friends and colleagues from the intelligence and security communities say that we will soon be visited by a "Cyber Pearl Harbor." I share this concern. The issue, however, is not whether government and private sector leaders recognize the threat. The threat is clear. The question is what do we do about it?

In the cyber realm, the US Government—from the White House and Department of Defense to the US Congress itself—has been unable to prevent many attacks on its systems. Meanwhile, US companies that employ millions of Americans are not only attacked by criminal organizations and lone wolf hackers, but also by Nation-States. Disruptions occur, business is being halted, data and proprietary information is being stolen, and our economy is being impacted. And many of our public and private networks are greatly interdependent.

At the end of the day, if we are not prepared to enable government and critical industries to share information and coordinate to prevent major cyber attacks and incursions, we will also be unprepared to respond together and to be resilient if and when attacks occur. In this sense, we are just as vulnerable to experience a "Cyber Katrina"—that is, experience a disaster on top of a disaster—as we are to realize a "Cyber Pearl Harbor."

Information sharing and public-private partnerships must be foundational to our national cyber security and resilience efforts. I applaud the President for issuing his Executive Order on Cybersecurity and for pursuing, through NIST, a public-private framework. This is a positive and important step. But I would caution against leveraging this process as merely a path toward prescriptive mandates.

In a world that sees data move at the blink of an eye, you will not be able to legislate or regulate fast enough to stop the evolving dangers we see—or do not see—in the cyber domain.

I know that some members favor a prescriptive approach to cyber security because of the legitimate concern that critical infrastructure will be impacted. But if we know that Nation-States and terrorist groups are probing and attacking the systems of our critical infrastructure operators, doesn't government have a responsibility to work with the private sector owners? And if government and private sector owner-operators are not collaborating, how will we determine the source of an attack or determine the proper course of action to take in a timely manner?

The game has changed. A 20th Century regulatory model simply will not work to combat this 21st Century threat. It requires both government and industry leaders to think anew. We need to support agile paradigms based on information sharing and public-private partnership.

The development of the cybersecurity framework is off to a good start. It has the potential to build balanced and sustained relationships between business and government so that individuals can experiment freely and quickly counter fast-paced threats to U.S. national security.

I highly recommend that Congress pass cyber bills that have earned widespread industry support, such as information-sharing measures, and refrain from codifying the cyber executive order before it has had the opportunity to demonstrate its efficacy. Lawmakers should conduct oversight of the presidential order to ensure that the private sector is an equal partner in its design and implementation.

As cyber threats grow, we can choose to repeat history. After a major incident, we can point fingers or issue voluminous post-mortem reports only to learn, as we did after 9/11 and after Katrina, that we needed more information sharing and collaboration are necessary between the public and private sectors.

Or, we can learn from history and do what needs to be done now. Enact Federal Information Security Act (FISMA) reform to get the government's own house in order. As the House has done on a wide bipartisan basis, pass information sharing legislation. Provide liability protections for private sector entities working with the government. Let's focus on areas of agreement and get legislation passed.

The adage, "We have faced the enemy and it is us," need not be the case.

Today we are facing numerous enemies in both the physical and cyber worlds. We need to face them together.

To be more specific, Mr. Chairman, I would like to expound upon some of the issues I have just summarized and make additional points to validate how successful public private partnerships have benefited our overall homeland security and why their application to our cyber challenges are relevant:

-The future of homeland security is tied to successful public-private partnerships, which has a lengthy history.

My experiences over the past decade and more tell me that the future of homeland security is closely tied to the success of partnerships between government and the private sector.

As you know, the protection of U.S. critical infrastructure has a lengthy history involving the business community. Issued in 1998, Presidential Decision Directive No. 63 (PDD-63) helped spur the protection of critical infrastructure and launch the formation of information sharing and analysis centers (ISACs) across the private sector. In 2003, Homeland Security Presidential Directive No. 7 (HSPD-7) updated the policy of the United States and the roles and responsibilities of various agencies related to critical infrastructure identification, prioritization, and protection.

Jumping forward a few years, 2006 witnessed the creation of the National Infrastructure Protection Plan (NIPP) and the Critical Infrastructure Protection Advisory (CIPAC). The NIPP resulted in the establishment of sector-coordinating councils (SCCs) and government-coordinating councils (GCCs) to work together on furthering the protection and resilience of the critical infrastructure community under the authorities of CIPAC. The NIPP was revised in 2009 to reflect an evolution of the process, including expanded integration of all-hazard and similarly important risk-management principles.

Businesses focus on guarding their operations from interruption, preventing the loss of intellectual property and sensitive customer data, and protecting public safety. Companies devote considerable resources toward maintaining their operations in the wake of a natural hazard or man-made threat, such as a terrorist attack. Business owners and operators understand it is imperative that critical infrastructure assets be well protected and resilient.

Issued on February 12, 2013, PPD-21, *Critical Infrastructure Security and Resilience*, calls on DHS to update the NIPP and deliver it to the president next month. At the same time, the administration is undertaking several homeland security-related initiatives simultaneously—including creating the cybersecurity framework, framework performance goals, and framework incentives. Each initiative, including reworking the NIPP, features one or multiple working groups in combination with tight deadlines, contributing to a flurry of activity.

Important elements of the business community—e.g., individual companies, SCCs, the Partnership for Critical Infrastructure Security (PCIS), and industry associations—dedicate vast resources toward engaging the government because it's in their best interests to do so. But they are also committed to advancing the common good of their communities and the nation.

-Policymakers should highlight public-private *successes* against America's adversaries in order to reinforce and replicate collaborative and innovative performances in the future.

a. Global supply chain security.

Businesses are linked together through a global web of interconnected, predictable, and efficient supply chains. American firms rely on these complex supply chains to access international consumers and compete in the global marketplace. Making improvements to

address cross-border friction would smooth the flow of trade and would ensure timely delivery of inputs and final products. Implementing such improvements would increase the competitiveness of U.S. businesses and unleash the potential for small- and medium-sized businesses to access foreign markets. DHS needs to review how these supply chains enhance U.S. businesses competitive advantage, and see how the department can reform and modernize their processes.

In the aftermath of September 11th, government officials and their private-sector counterparts came together to strengthen supply chain security, including developing the Customs-Trade Partnership Against Terrorism (C-TPAT). Together, both sides stepped up, invested in the program, and solved many of the mutual problems faced by government and the private sector.

Similarly, in the wake of the printer cartridge bomb plot on October 29, 2010, the private and public sector worked together to develop the Air Cargo Advance Screening (ACAS) pilot. The pilot program was up and running within two months of the terrorist attempt, and it closed gaps in security to ensure it could never happen again. Just as important, the ACAS program was flexible and fit existing business processes to ensure that businesses were not overburdened with mandates.

The public and private sector have interests that align much of the time. The challenges are finding those areas of commonality, and working together to develop a plan or program that promotes U.S. economic and physical security. Finding common ground should not always take a crisis to facilitate. We should be working with the private sector to facilitate trade, travel, ports, and supply chains to enhance to competitiveness of industry, so that when a crisis does come, we have the appropriate people working together to respond.

In the next 10 years, I hope to see the public and private sector relationships in homeland security go to the next level, where they work together to modernize our borders, our emergency response capabilities and other areas of the DHS mission, to a place where the private sector is viewed as a partner in homeland security, rather than just the "regulated" party.

I recommend that the United States reach out to its trading partners to develop a comprehensive, multilateral supply chain security program that promotes trade and security on both sides of the transaction. The United States can accomplish these goals by furthering discussions via the World Customs Organizations SAFE Framework and moving forward on Mutual Recognition Arrangements (MRAs) with key trade partners. Businesses harmonize processes around the globe and governments should as well.

Also, the U.S. should set the global example for border management, and present a "one-government" approach to border management. This would happen when all government border agencies work together to facilitate the legitimate flow of trade. Multiple agencies unsurprisingly have duplicative mandates, data requirements, and approaches to clearing goods. This is inefficient and ineffective for both the private and public sector. U.S. Customs and Border Protection (CBP) have taken steps to promote their "Trade Transformation Agenda" that includes this and other major trade and security priorities. These efforts and encourages the agency to deliver commercially meaningful results.

Congress would do well to support funding CBP for 3,500 additional customs officers at the ports of entry to improve security, trade, and travel facilitation. The dual role of CBP is to secure our homeland and facilitate trade and travel. Over the past five years, a disproportionate amount of funding has been designated for increasing staffing of border patrol officers between the ports of entry. These efforts seem reasonable, but more funding needs to be devoted towards customs officers at ports of entry.

Related, commercial and pedestrian border crossings suffer from understaffing which increases wait times, costs industry billions, and discourages travelers and trade from approaching the border. Investing in staffing at the ports of entry would enhance security, facilitate trade, and improve travel for the millions of business and leisure travelers entering the United States every year.

b. Chemical security.

Under the Chemical Facility Anti-Terrorism Standards (CFATS) program, U.S. businesses will commit billions of dollars toward measures approved by the Department of Homeland Security (DHS) to make chemical facilities more secure and resilient in an all-hazards context. CFATS is a relatively new example of public-private partnership in the context of homeland security, which is why it is important for policymakers to take industry views into consideration as the program takes shape. Although revelations about mismanagement of the CFATS program have been a concern, the concepts underpinning the program remain sound.

The tragedy at the West Fertilizer Company facility shows that we need to redouble our public-private efforts to bring so-called outlier sites into CFATS. DHS needs appropriate resources to administer the program in a timely fashion. Ultimately, to enhance security at chemical facilities, Congress should pass legislation authorizing a clean, long-term extension of CFATS, and avoid proposals that would add layers of complexity and costs on businesses.

Genuine Public-Private Partnerships are necessary to meet our cybersecurity challenges

a. The Cyber Framework

As mentioned previously, the cybersecurity framework under development has the potential to build balanced and sustained relationships between business and government so that individuals can experiment freely and quickly counter fast-paced threats to U.S. national security. It is constructive that the National Institute for Standards and Technology (NIST) has been given the responsibility to coordinate an environment where technical and security professionals come together to identify the most applicable and effective guidance throughout industry sectors and promote its implementation.

I agree with comments made by Patrick Gallagher, Under Secretary of Commerce for Standards and Technology at the Department of Commerce, who testified in March before the Homeland Security and Commerce committees that a NIST-coordinated and industry-led framework would "draw on standards and best practices that industry is already involved in

developing and adopting," and would "ensure a robust technical underpinning to the framework." He emphasized that a multi-stakeholder approach would take advantage of the strengths of the public and private sectors to develop solutions that both sides would find beneficial to security. Under Secretary Gallagher said that the "approach does not dictate solutions to industry, but rather facilitates industry coming together to offer and develop solutions that the private sector is best positioned to embrace."

Critical infrastructure entities identified under cybersecurity executive order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*, should be the primary voices behind the development of the cybersecurity framework. In turn, the administration has a unique opportunity to collaborate with the private sector as components of the EO are being developed and put into practice.

It is significant that S. 1353, the "Cybersecurity Act of 2013," stopped short of codifying elements of the EO, because it is constructive to let framework efforts play out fully before they are written into law.

b. Information Sharing Bill

Developing the framework is only one piece of the cybersecurity puzzle. I urge Congress to focus on improving information sharing and liability protections, encouraging international cooperation against cybercrime, enhancing national cybersecurity R&D, reforming the Federal Information Security Management Act of 2002 (FISMA), and heightening public awareness and education.

Of particular importance, Congress should pass a cybersecurity bill to improve the exchange of cyber threat information between business and government to elevate overall situational awareness in a manner that's sustainable. Legislation needs to help put timely, reliable, and actionable information into the hands of business owners and operators so that they can better protect their systems and assets against the increasing threat of cyberattacks.

Legislation should support existing information-sharing and analysis organizations and incorporate lessons learned from pilot programs and exercises undertaken by critical infrastructure sectors. They offer complementary, demonstrated models for enabling the government to share actionable cyber threat information with the private sector—thereby affording security professionals the opportunity to implement measures intended to reduce a business' cyber risk profile—without creating burdensome regulatory mandates or new bureaucracies.

In addition, businesses need certainty that threat and vulnerability information voluntarily shared with the government would be provided safe harbor and not lead to frivolous lawsuits, would be exempt from public disclosure, and could not be used by officials to regulate other activities. Legislation also needs to include an exemption from antitrust laws, which limit exchanges of information between private entities, in order to help prevent, investigate, and mitigate threats to cybersecurity.

Further, executive action, like legislation, must focus not only on strengthening U.S. critical infrastructure but on encouraging innovative cybersecurity practices. Policymakers need to help the law enforcement community increasingly shift the cost of cyber intrusions to nefarious actors, which the business community and government both confront daily.

Conclusion

In a post 9/11 environment, the government has to be mindful that they are not the only interests with skin in the homeland security mission. The private sector owns and manages the majority of critical infrastructure, and its facilities are vital to the economic security of this country. The United States cannot solve myriad global threats by regulating the business community.

DHS needs to work collaboratively with the private sector to nurture business solutions to the security challenges that face this country. When a natural hazard or bad actor threatens our nation, the private sector has vested interest in ensuring that the incident is mitigated successfully or prevented and that the business community is resilient. Thus, policymakers should focus on public-private successes—including in the areas of global supply chain security, chemical security, and cybersecurity—against America's adversaries in order to reinforce and replicate special and innovative performances in the future.

Once again, I greatly appreciate the opportunity to testify today and look forward to working with the committee on these and other issues. Thank you very much.

###