Statement for the Record
Robert B. Stephan,
Assistant Secretary, Infrastructure Protection
National Protection and Programs Directorate
Department of Homeland Security

Before the

Committee on Homeland Security and Government Affairs
Subcommittee on State, Local and Private Sector Preparedness and Integration
United States Senate

Thursday, July 12, 2007
2:00 p.m.
Dirksen Senate Office Building, Room SD-342

Thank you, Chairman Pryor, Senator Sununu, and distinguished members of the Subcommittee. I appreciate this opportunity to address you on the role of the Department of Homeland Security (DHS) Office of Infrastructure Protection (OIP) in ensuring robust coordination with the private sector as we work together to protect our nation's critical infrastructure and key resources (CI/KR) and strengthen national CI/KR-related "all-hazards" incident management capabilities.

My staff and I are keenly aware of the importance of fully integrating and working with our private sector partners across our mission space. As a point of departure, it is important to note that the vast majority of our nation's critical infrastructure—approximately 85 percent—is owned and operated by private sector entities. Hence, our comprehensive work with the private sector represents a key component of our national CI/KR information sharing network and protective architecture. Both Congress and the President have recognized that, as a Nation, the full support, cooperation, and engagement of Government and private sector partners at all levels is required to prevent terrorist attacks, mitigate natural or manmade disasters, restore essential services in the aftermath of an incident, and maintain the American way of life.

I know you recently heard from R. David Paulison at the Federal Emergency Management Agency (FEMA) and Al Martinez-Fonts of the DHS Private Sector Office during Part One of this hearing. My office works very closely with both FEMA and the Private Sector Office in a collaborative approach to building and supporting this important public-private partnership. We have worked collaboratively to strengthen our incident management relationship with the private sector, building on important lessons learned during the 2005 hurricane season.

Our partnership with the private sector spans the diverse spectrum of the 17 CI/KR sectors identified in Homeland Security Presidential Directive-7 (HSPD-7). This partnership also extends to high-risk communities across the country, where we have focused a great deal of effort to bring together Federal, State and local government and private sector partners to conduct a variety of CI/KR-related activities such as vulnerability assessments, security planning, information sharing, best-practices exchanges, risk reduction, and incident management. This partnership, in fact, forms the operational core of our National Infrastructure

Protection Plan (NIPP) and its supporting Sector Specific Plans (SSPs) in each of the 17 CI/KR sectors.

I would like to take this opportunity today to provide you with specific examples of the progress the Department of Homeland Security has made over the past four years towards meeting the challenge of building and sustaining the comprehensive framework required to protect and enhance the resiliency of our nation's CI/KR in an all-hazards context. My remarks will focus on the following major topics:

- Roles and responsibilities of the Office of Infrastructure Protection;
- CI/KR protection framework detailed in the NIPP and its supporting SSPs;
- NIPP public-private sector partnership and information sharing model;
- NIPP risk management framework and protective programs that drive private sector coordination; and
- CI/KR dimension of our domestic incident management framework.

Roles and Responsibilities of the Office of Infrastructure Protection

Since its inception in March, 2003, the mission of the DHS Office of Infrastructure Protection has been clear. Our overall approach is focused on establishing and sustaining a risk-based, unified program to protect and enhance the resiliency of our nation's CI/KR. The key to this approach is the successful integration of diverse authorities, resources, and capacities across a broad universe of functional agencies, governmental jurisdictions, and private industries to achieve a "layered defense" of physical protection, cyber security, and resiliency within the 17 CI/KR sectors.

This is a long-term effort that involves comprehensive government and private sector collaboration inside and outside of regulatory space at various levels across our national risk landscape. For its part, the private sector has made substantial investments to strengthen physical and cyber security, boost resiliency, increase redundancy, and develop contingency plans since the September 11th attacks. State and local agencies have also stepped up to the plate in many important ways to strengthen their ability to support the CI/KR protection mission within their jurisdictions. Supporting these efforts, the Department has provided nearly $2 billion in CI/KR-targeted risk-based grant funding – including $445 million this year – to deter threats, reduce vulnerabilities, minimize consequences, and build resiliency across our nation's most at-risk CI/KR.

The basic charter of the Office of Infrastructure Protection is to provide the coordinating leadership required at the national level to build and sustain a very complex, dynamic, and diverse protection partnership that drives unity of effort across the 17 CI/KR sectors. In our OIP FY08-13 Strategic Plan, we have identified six primary goals essential to implementing our national mission:

- Build and sustain effective CI/KR partnerships and coordination mechanisms;

- Understand and share risk and other information about terrorist threats and other hazards to the nation's CI/KR;
- Build and implement a sustainable, national CI/KR risk-management program;
- Ensure efficient use of resources for CI/KR risk management;
- Provide a foundation for continuously improving national CI/KR preparedness; and
- Promote a culture of organizational excellence and a quality work environment that values and supports the workforce.

CI/KR Protection Framework Detailed in the NIPP and Its Supporting SSPs

The guiding force behind our strategic planning and resource allocation activities is the National Infrastructure Protection Plan, or NIPP. I am pleased to report that we marked a significant milestone on June 30th of this year–the first anniversary of the issuance of the NIPP, our strategic national blueprint for the CI/KR mission area that was, in fact, developed through the public-private partnership framework. The achievements that I will discuss with you today are a direct result of the commitment, dedication, and teamwork that characterizes this framework.

Through the NIPP, we now have a unified national game plan and an ever expanding arsenal of tools with which to implement our mission. The NIPP establishes the overall risk-based construct that defines the unified approach to protect and enhance the resiliency of the nation's CI/KR in an all-hazards context. This construct applies to "steady-state" risk reduction activities across the sectors and also sets the stage for important CI/KR-related response and recovery activities under the National Response Plan (NRP).

Organizationally, the heart of the NIPP is the sector partnership model that establishes Sector Coordinating Councils (SCCs), Government Coordinating Councils (GCCs), and cross-sector coordinating councils to create an integrated national framework for CI/KR preparedness, protection, response and recovery across sectors and levels of government. This partnership model also forms the backbone of the networked approach to sharing information. A robust system for information sharing provides for multidirectional CI/KR-related exchanges of actionable intelligence, alerts, warnings, and other information between the various NIPP partners, including: Federal agencies, State and local agencies, CI/KR owners/operators, and sector-based information-sharing entities.

The NIPP partnership model encourages CI/KR owners and operators to create or identify an SCC as the principal entity for coordinating with the government on a wide range of CI/KR protection activities and issues. SCCs are self-run and self-governed; specific membership varies from sector to sector, reflecting the unique composition of each sector. The guiding principle for SCCs is that membership is structured to be representative of a broad base of owners, operators, associations, and other entities – both large and small – within a sector.

GCCs serve as the government counterpart for each sector to enable interagency and cross-jurisdictional coordination. GCCs are comprised of representatives from across various levels of government and functional disciplines as appropriate to the security landscape of each sector. Each GCC is chaired by a representative from the designated Federal Sector-Specific Agency and co-chaired by myself, as the Assistant Secretary for Infrastructure Protection.. Together, the

SCCs and GCCs provide a forum through which NIPP security partners may engage in a broad spectrum of activities, such as: security planning, policy coordination, exercise planning, risk methodology coordination, implementation of protection initiatives, information sharing, and incident management.

The "glue" that binds this partnership together is the NIPP "value proposition" that articulates guiding principles for coordination and cooperation between government at all levels and the private sector. In accordance with these principles, DHS is committed to:

- Providing owners and operators with timely, accurate, and actionable all-hazards information;
- Ensuring that owners and operators are engaged at senior executive and operational levels in key planning, policy, requirements, and resource allocation discussions;
- Articulating the benefits of a risk-based, cross-sector approach to preparedness, resilience, and protection;
- Working with owners and operators to clearly establish risk-based priorities for prevention, protection, and recovery;
- Providing specialized technical and planning expertise to support CI/KR-related preparedness, protection, and recovery; and
- Coordinating with CI/KR owners and operators on priorities, risk assessments, mitigation, and restoration and recovery activities in the context of incident management.

The finalization and release of the NIPP Sector-Specific Plans (SSPs) in May of this year represents another important milestone and illustrates the effectiveness of the NIPP Partnership Framework, which is, interestingly enough, a purely voluntary structure. Developed under the umbrella of this Framework, the SSPs represent adaptations of the NIPP baseline risk analysis and risk management approach, governance structure, and information sharing network as tailored to the specific needs and requirements of each of the 17 CI/KR sectors. This undertaking represents the first time that the Government and private sector have come together on such a large scale – literally across every major sector of our economy – to develop joint plans for how to protect and ensure the resiliency of our CI/KR against both terrorist incidents and natural disasters.

The development of the SSPs was, in fact, a comprehensive and dynamic undertaking that brought together thousands of public and private sector organizations across the 17 CI/KR sectors. The direct involvement of CI/KR owners and operators, State and local government agencies, trade associations, professional organizations, and other security partners was inherent to this process. As part of this effort, my office conducted six technical assistance sessions during the 180-day SSP development process to address selected topics such as the incorporation of research and development requirements, information sharing networks and protocols, and the sharing of best practices across sectors. Each sector devised its own preferred approach for developing its plan and was required to ensure inclusion of a full slate of sector security partners. Many sectors conducted multiple review cycles, resulting in a robust consideration of sector partner comments and, ultimately, a more complete and inclusive end product. The overall magnitude of comments across the sectors was indicative of the degree of interest in and the importance of this effort. An estimated 10,000 individual comments were received and

adjudicated, which is roughly the same number of comments processed during the development of the NIPP Base Plan.

In a series of parallel undertakings, we are also leveraging the NIPP Sector Coordinating Council structure to develop sector guidelines for pandemic influenza preparedness, establish CI/KR protection research/development and modeling/analysis requirements, build a national CI/KR protection awareness and training program, and provide for expanded private sector participation in the DHS National Exercise Program (to include the upcoming Top Officials (TOPOFF) 4 exercise).

NIPP Public-Private Sector Partnership and Information Sharing Model

The NIPP partnership framework is enabling marked progress in another important area—information sharing. In accordance with the NIPP, we are currently implementing a networked approach to information sharing that constitutes a dramatic shift from a strictly hierarchical approach, that is, the Federal government sharing information down.. This networked approach allows distribution and access to information both horizontally and vertically using secure networks and coordination mechanisms, allowing information sharing and collaboration within and among sectors. It also enables multi-directional information sharing between government and industry that focuses, streamlines, and reduces redundant reporting to the greatest extent possible. Security partners are finding immediate value in tactical activities that incorporate sector-specific subject matter expertise. These processes are enabling the integration of the private sector security partners, as appropriate, into the intelligence cycle and National Common Operating Picture. Moreover, sector security partners are becoming more confident that the integrity and confidentiality of their sensitive information can and will be protected and that the information-sharing process can produce actionable information regarding CI/KR threats, incidents, vulnerabilities, and potential consequences.

Our efforts to enhance the sharing of information related to terrorism with the owners and operators of CI/KR have been integrated into broader efforts to establish the Information-Sharing Environment (ISE) as directed by the President in accordance with the Intelligence Reform and Terrorism Prevention Act of 2004. The purpose of the ISE is to measurably improve information sharing between and among Federal, State, local, and tribal governments; and between government agencies and private sector entities. In recognition of the important work underway in this area under the NIPP framework, the Program Manager of the ISE, in coordination with the Information Sharing Council, has officially designated the NIPP Partnership Framework coordinated through the Office of Infrastructure Protection as the Private Sector Subcommittee of the Information Sharing Council. In this role, the NIPP Partnership Framework provides an avenue for the private sector to engage in ISE-related policy, planning, and operational coordination, as well as a forum for identifying and satisfying information requirements originating from private sector security partners.

The CI/KR owners and operators utilize a number of mechanisms that facilitate the flow of information, mitigate obstacles to voluntary information sharing by CI/KR owners and operators, and provide feedback and continuous improvement regarding structure and process. These include the SCCs/GCCs, National Infrastructure Coordinating Center (NICC), Sector-level

Information Sharing and Analysis Centers (ISACs), OIP Sector Specialists, OIP Protective Security Advisors, DHS Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), and State and Major Urban Area Fusion Centers. These mechanisms accommodate a broad range of sector cultures, operations, and risk management approaches and recognizes the unique policy and legal challenges for full two-way sharing of information between the CI/KR owners and operators and government, as well as their unique requirements for efficient operational processes.

NIPP Risk Management Framework and Protective Programs that Drive Private Sector Coordination

During a situation or crisis, the ability to share concise and focused information with all those who need access to it is essential. To accomplish this end, the National Infrastructure Coordinating Center (NICC) was created as our 24/7 watch center focal point for coordination and communication with the CI/KR sectors. The NICC leverages the Homeland Security Information Network—Critical Sectors (HSIN-CS) as a mechanism to push information to private sector CI/KR owner-operators. The NICC has posted more than 800 threat assessments, situation reports, daily updates, and analysis documents within the past year, including pre-season CI/KR hurricane impact analyses produced by OIP's National Infrastructure Simulation and Analysis Center (NISAC).

Another important advancement in our relationship with the private sector is the establishment of the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), an infrastructure-intelligence fusion center that we operate jointly with the DHS Office of Intelligence and Analysis (I&A). Working in partnership with members of the U.S. Intelligence Community and national law enforcement agencies, HITRAC analyzes and monitors risks to domestic CI/KR, allowing our Office to provide actionable assessments and risk reduction recommendations to our sector security partners at both the classified and unclassified levels. Access to classified information and discussions is permitted through a security clearance sponsorship program in which we have provided SECRET-level clearances to more than 900 private-sector officials across the 17 CI/KR sectors.

Through HITRAC and the NICC, private sector security partners receive a thorough combination of real-time threat, situation, and status information and analyses which, in turn, is used to inform security and operational planning, resource investments, and key risk mitigation activities. Private sector liaison personnel, on-call subject matter experts, and other organizations – including, but not limited to, the National Coordinating Center for Telecommunications, SCCs, GCCs, and ISACs – are utilized by HITRAC and the NICC in order to help inform comprehensive analyses of all-source information, and provide timely threat and warning products as well as a variety of more strategic level assessment products.

Collaborating with other key stakeholders through the NIPP Partnership Framework is fundamental to the success of numerous important national CI/KR-related risk reduction initiatives—to include important "boots-on-the-ground" activities—that DHS has implemented during the last four years. Examples of these activities include following:

Comprehensive Reviews – This initiative involves a structured, joint analysis of Federal, State, local, and private sector capabilities needed to enhance the security of our highest-risk national CI/KR. Recommendations to mitigate the effects of a potential terrorist attack, natural disaster, or other emergency on these infrastructures as well as an ability to target Federal CI/KR protection grants against gaps identified are provided through this program. To date, we have conducted 64 comprehensive reviews involving both the Chemical and Nuclear Sectors. The Chemical Sector Comprehensive Review Team conducted analyses of six regions that included nine states and Federal grant funding of $25 million. The Nuclear Sector Comprehensive Review Team conducted 58 comprehensive reviews that provided the basis for additional security improvements within the Nuclear Sector through the Buffer Zone Protection Program.

Buffer Zone Protection Program (BZPP) – The BZPP is a DHS-administered grant program designed to help local law enforcement and CI/KR owners and operators increase security within the "buffer zone," the area outside of a facility that can be used by an adversary to conduct surveillance or launch an attack. This program provides a coordinated process to identify and assess vulnerabilities, conduct security planning, implement preparedness activities, coordinate protective measures, and obtain mitigation equipment needed to enhance security. More than 2,200 BZPP site visits, 181 planning workshops, and 176 technical assistance visit engagements have taken place since 2004 in locations around the country. DHS has distributed approximately $190 million in grants to our State and local law enforcement security partners in order to improve the overall security posture of these high-risk areas and to refine and strengthen locally generated CI/KR protection plans.

Site Assistance Visits (SAVs) – The SAV program provides a collaborative process for conducting information-gathering visits in support of several key objectives, such as gaining a better understanding and prioritization of CI/KR vulnerabilities and increasing owner and operator awareness of threats and vulnerabilities. These visits are conducted jointly by DHS, other Federal, State, and local government entities, and CI/KR owners and operators. Through this program, we provide CI/KR owners and operators with options for increasing their ability to detect and prevent terrorist attacks and recommendations for reducing infrastructure vulnerability. Information derived from these visits is used to produce Common Vulnerabilities, Potential Indicators of Terrorist Activity, and Protective Measures reports that are available to Federal, State, local, tribal, and private sector partners through our information-sharing network. In the last two years, we have conducted a total of 700 Site Assistance Visits, with an aggressive schedule for many more through the end of FY 2007 and into FY 2008.

Protective Security Advisors (PSAs) – PSAs represent a critical in-place "boots on the ground" capability in high-risk areas around the country. Although we do a great deal of planning and coordination here in Washington, D.C., CI/KR-related program implementation, partnership interaction, and performance feedback are more appropriately driven home at the local level. Recognizing this fact, DHS has permanently stationed 78 PSAs strategically throughout the country to enhance CI/KR protection efforts and stakeholder interaction. These trained protective security experts foster, build, and maintain partnerships with State, local, and tribal governments, community leaders, CI/KR owners and operators, and local-level businesses on a daily basis. PSAs coordinate requests from CI/KR owners and operators for services and resources, including Soft Target Awareness Courses (STACs), Surveillance Detection (SD)

training, vulnerability assessments, security planning sessions, and technical assistance visits. To date, PSAs have conducted more than 15,000 liaison visits with State, local, and private sector partners. They have also provided support to the 2,200 Buffer Zone Protection Program planning efforts; 6 Chemical Sector Comprehensive Reviews, 54 Nuclear Sector Comprehensive Reviews, and participated in approximately 500 Site Assistance Visits. .

PSAs are the first Office of Infrastructure Protection personnel to respond to incidents within their area of responsibility. PSAs provide crucial situational awareness during times of crisis or special events, including Hurricanes Katrina, Ophelia, Rita, and Wilma; the Virginia Tech shootings; and the ongoing flood and wildfire events in the Midwest and Pacific Coast. They are also engaged in security planning and situational awareness activities supporting special events such as the Super Bowl, Indianapolis 500, 2010 Olympics, and so forth.

Multi-Jurisdiction Improvised Explosive Device (IED) Security Plans – The Multi-Jurisdiction IED Security Planning process assists security partners in high-risk urban areas and other locations throughout the United States in developing thorough bombing prevention and response plans. These plans are intended to integrate assets and capabilities from multiple jurisdictions and emergency service disciplines. As part of this program, to date we have conducted more than 17 security plan development sessions for high risk port facilities around the country. These efforts have focused on enhancing port security preparedness for a potential terrorist attack using Underwater Hazardous Devices (UHDs). The multi-jurisdictional IED Security Planning workshop provides participants with a comprehensive, tailored annex to the Area Maritime Security Plan that details the prevention of, response to, and recovery from, a UHD attack.

Technical Resource for Incident Prevention (TRIPwire) – TRIPwire is an online, collaborative, information-sharing network designed to support bomb squads and other law enforcement officials. It provides users with information about current terrorist bombing tactics, techniques, and procedures, including IED design and placement. By combining expert analysis and reports with relevant documents, images, and videos gathered directly from terrorist sources, TRIPwire helps operators anticipate, identify, and prevent bombing incidents. TRIPwire is provided via a secure, restricted access Internet portal free of charge to qualified bombing prevention and law enforcement community personnel. TRIPwire currently has more than 1,800 users, including 566 certified bomb technicians, and has the potential to reach more than 500,000 emergency services personnel. Current users represent 40 Federal departments and agencies, 28 military units, 365 State and local agencies, and 35 private sector companies and organizations. Since June 2006, TRIPwire has received nearly 4,000,000 site hits.

Soft Target Awareness (STAC) and Surveillance Detection (SD) Training – The STAC is a week-long course that provides private sector facility managers, supervisors, and security and safety personnel with a venue to receive and share baseline terrorism awareness, prevention, and protection information and is intended to enhance individual and organizational security awareness. SD Training is a three-day course that provides a guideline for mitigating risks to CI/KR through developing, applying, and employing protective measures and the creation of a surveillance detection plan. OIP has provided 284 STACs across 71 cities and 97 SD Trainings within a wide variety of locations around the country.

NIPP Awareness Level Training Program – Since being put online in late-December 2006, this web-based training program has been accessed by more than 1,000 security partners each month. Developed in coordination with the FEMA Emergency Management Institute, this program offers NIPP training free of charge to all security partners, including private sector owners and operators. Recently, a classroom version of the course was developed, and participants have the option of completing either the web-based training program or the classroom program for continuing credit. Companion training videos have also been created for use across various venues to explain the NIPP; each video includes testimonials from several key private sector partners.

CI/KR Dimension of Our Domestic Incident Management Framework

In the aftermath of the 2005 hurricane season, we have worked very closely with Federal, State, and local incident managers and private sector entities to build out a robust CI/KR incident management framework and operational capability. We have collaborated extensively with the National Operations Center (NOC) and now provide direct day-to-day representation and coordination of key CI/KR functional elements for the NOC. We also maintain full-time OIP representation on the DHS Incident Management Planning Team and at the FEMA National Response Coordination Center (NRCC). This representation ensures that CI/KR inputs, interests, and concerns are accurately presented and included in the development of both the National Common Operating Picture and Federal Interagency Contingency Plans – based on the 15 National Planning Scenarios – through detailed CI/KR annexes. These OIP representatives also ensure the incorporation of CI/KR interests into other contingency plans, such as hurricane season preparedness plans, and NRP activation for incidents that require Federal involvement.

In another area, OIP is engaged in multiple planning and information-sharing initiatives with CI/KR owners and operators to ensure the integrity of the nation's CI/KR in the event of an influenza pandemic. These efforts support the DHS overarching responsibility for coordination of Federal response activities. The Pandemic Influenza CI/KR Preparedness, Response, and Recovery Guide was completed in 2006 and posted to the www.pandemicflu.gov and www.ready.gov websites. Continuing this effort, we are now actively engaged in additional activities to stimulate and support CI/KR pandemic preparedness. A comprehensive process to develop 17 sector-specific guidelines in collaboration with each of the SCCs and GCCs is currently underway. These guidelines, which are expected to be completed by early fall, will provide comprehensive, sector-unique planning information for our security partners. Once completed, these guidelines will be posted to Federal and industry websites and widely disseminated to businesses. Additionally, over the past year, we conducted workshops and forums to identify issues and gaps in CI/KR pandemic influenza planning. Multiple pandemic influenza preparedness workshops are planned over the next 12 months to continue the dialogue between CI/KR owners and operators and their community, State, local, tribal, Territorial, and Federal partners.

In support of our evolving incident management roles and responsibilities, OIP is focusing a great deal on training and exercise programs to test our exiting coordination capabilities, information sharing network, and overall readiness. We have significantly raised our level of readiness to provide CI/KR support for incident management through our training and exercise

programs, each of which is fully compliant with the Homeland Security Exercise and Evaluation Program (HSEEP). The CI/KR sectors are actively planning for participation in the DHS-led TOPOFF 4 full-scale national exercise in October 2007. This exercise will test our analysis and coordination processes and provide a venue for government and private sector leaders to verify and validate our preparations for a catastrophic terrorist attack. Several hundred private sector partners participated in the TOPOFF 3 exercise in 2005, and we expect even greater participation for the upcoming TOPOFF 4 event.

In addition to OIP and DHS specific readiness, OIP also focuses on Sector-Based readiness activities. The NICC recently disseminated a series of documents to the CI/KR Sectors to support sector preparedness efforts for the 2007 hurricane season. These products included: 1) the 2007 scenario-driven NISAC hurricane impact analysis products that address potential CI/KR impacts in a number of high-risk geographic regions and 2) updated protocols for incident-related CI/KR sector impact assessment and status reporting, information-sharing, and requests for information and assistance. Additionally, the NICC hosted two training workshops for the Federal Sector-Specific Agencies to refine public-private sector reporting processes prior to the 2007 hurricane season. The NICC also conducts monthly reporting drills with the SSAs and more frequent drills with the National Operations Center (NOC).

Finally, in response to significant CI/KR security events such as the foiled airline bombing plot in the United Kingdom last August, the recent JFK Airport bombing plot, and the recent attempted bombing events in London and Glasgow, OIP convened conference calls with the SCCs to share critical information and recommendations regarding these situations as they developed with our private sector partners.

Currently, we are finalizing OIP's long-term strategy for continued program growth and evolution. This effort is being conducted in tandem with the Sector Annual Reporting process under the NIPP. Our goal is to continue our risk-based approach to CI/KR protection, tailored to the needs and requirements of the 17 CI/KR sector. As we move into the future, the NIPP Partnership Framework and the thousands and thousands of security partners it brings together will continue to drive our national approach. No one can predict the future with 100% accuracy but certain things are a given—technology, the ways CI/KR owners and operators do business, and their supply chain dependencies will evolve, and vulnerabilities and consequences will change accordingly. In effect, we can count on our risk calculation changing in a dynamic fashion over time. Another fact is very clear—we know that we face a clever, flexible, patient, and determined terrorist adversary. The path forward provided by the NIPP, the SSPs, and the NIPP Partnership Framework will continue to serve us well and allow us to act collaboratively to adapt to a dynamic risk environment and achieve national unity of effort.

Success over time means making commitments and following through with them. We will approach our collaborative implementation of the NIPP and SSPs with this in mind and continue to refine and enhance our solid relationship with the private sector. I will leave you with one more important observation—the more we utilize the Sector Partnership Framework for the appropriate purposes, the stronger and more effective it gets. We continue to incorporate lessons learned from interactions on various relevant issues that enable continuous improvement and adaptation of partnership communication and coordination.

The NIPP and its supporting SSPs chart the path forward for continuous improvement in the security and resiliency of our critical infrastructure. Continued support of the focused activities of OIP in concert with all of our CI/KR partners will help ensure our preparedness in this critical mission area.

Thank you for this important opportunity to discuss the CI/KR protection mission area and the public-private sector partnership framework that lies at its core. I would also like to thank you for your continued support and dedication to the success of this vital component of the overarching homeland security mission. I would be happy to answer any questions that you may have at this time.