Statement for the Record
James L. Snyder
Deputy Assistant Secretary for Infrastructure Protection
National Protection and Programs Directorate
Department of Homeland Security

Before the
United States House of Representatives
Committee on Homeland Security
Subcommittee on
Transportation Security and Infrastructure Protection

"The Mumbai Attacks: A Wake-Up Call for America's Private Sector"

March 11, 2009

Thank you, Chairwoman Jackson Lee, Ranking Member Dent, and Members of the Subcommittee. I appreciate the opportunity to participate in the hearing "The Mumbai Attacks: A Wake-Up Call for America's Private Sector," and to discuss the Department of Homeland Security's Office of Infrastructure Protection's interaction with our government and private sector partners during and following the terrorist attacks in Mumbai, India.

As acknowledged with this hearing, the Mumbai attack on November 26-30, 2008, served as a strong reminder that the threat of terrorism remains very real, and that those who wish us harm remain dangerous and adapt quickly to changing circumstance. The terrorist attacks were well-planned, well-coordinated, and well-executed. The terrorists carried out a complex attack and struck multiple targets in the transportation and commercial facilities sectors, particularly hotels and religious locations. One example of their ability to adapt was their decision to shift tactics and conduct a water-borne entry rather than the normal overland entry to the target area, thus avoiding observance. Their attacks were also facilitated by the targets' business requirements for open access, a reality that represents an inherent security challenge. This type of attack highlights the vulnerabilities of soft targets, and how difficult it is to prepare, prevent, and respond to such attacks.

Consequently, we too must adapt to this dynamic threat environment—as well as to the dangers posed by catastrophic natural events—by remaining both nimble and flexible in our approach to infrastructure protection, and by continuing to enhance our coordination efforts with government at all levels and with the private sector.

IP activities are based on the framework and approach outlined in the National Infrastructure Protection Plan (NIPP). Our mission is to work closely with our government and private sector partners across the 18 critical infrastructure and key resources (CIKR) sectors and to lead the effort to ensure that a comprehensive, multi-

faceted framework exists to secure and enhance the resiliency of the nation's CIKR. Because the majority of the Nation's CIKR are owned and operated by the private sector, the Department must leverage partnerships and relationships to achieve success. Using the NIPP framework, the Department has successfully established primarily voluntary partnerships among interested Federal, state, local, tribal and private sector entities. These partners work within the framework to set goals and priorities, identify key assets, assign roles and responsibilities, allocate resources, and measure progress against national priorities. DHS released the NIPP in 2006 and, following its first triennial review and update, recently re-released it as the 2009 NIPP. The subtitle of the 2009 NIPP is "Partnering to Enhance Protection and Resiliency."

The value of the relationships we have built through this partnership has been demonstrated in local and national response to hurricanes, fires, and other real world incidents. In the steady-state environment, we sustain these relationships through information sharing, exercise, and training so that when an incident occurs, whether man-made or natural, we can respond and recover effectively and efficiently. For example, on December 9, 2008, IP hosted a tabletop exercise based on a multiple improvised explosive device attack with representation from all 18 critical infrastructure sectors. Additionally, IP's Commercial Facilities Sector Specific Agency Executive Management Office (SSA-EMO) participated in a January 29, 2009, Terrorism Simulation Exercise. The tabletop exercise, Threat & Response Options – Public Communications Challenges, was conducted with the Commercial Facilities Real Estate Roundtable subsector. The exercise was designed around a Mumbai-style attack and facilitated active discussion on preventive, response, and recovery activities. These are only two of many exercises we conduct annually with our CIKR partners that build the relationships and processes we use during response to all-hazards events.

In the case of Mumbai, IP worked directly with the Commercial Facilities Sector, Banking and Finance Sector, Transportation Sector, and leadership from religious organizations to share relevant information. To facilitate information collection, analysis, and distribution, IP leveraged the incident management capabilities built into its Incident Management Cell (IMC). The IMC is a cross-functional operations group that provides the core staff and facilities around which IP's scalable incident management capability coalesces during a large-scale CIKR incident. Prior to the Mumbai incident, the IMC provided effective leadership and coordination in communicating with our partners during Hurricanes Gustav and Ike. IP's response is guided by the National Response Framework and National Incident Management System which enable a systematic approach to response operations.

IP's initial actions on the first day of the Mumbai attacks, November 26, were to disseminate Common Vulnerabilities (CV), Potential Indicators of Terrorist Activity (PI), and Protective Measures (PM) Reports to public and private sector partners through the Homeland Security Information Network for Critical Sectors (HSIN-CS) portal and its 4,500 member user community. These reports provide security officials with specific information on potential vulnerabilities and recommendations on specific protective measures that they can implement to increase their security posture.

On November 27, IP released a TRIPwire Significant Incident Report (SIR) to provide information on the attacks to over 6,000 users in the TRIPwire community. TRIPwire is the Department's online, collaborative, information-sharing network for bomb squads, law enforcement, and other emergency services personnel. It provides continuously updated information about current terrorist improvised explosive device (IED) tactics, techniques, and procedures, including design and emplacement techniques. IP issued three additional TRIPwire postings over the next 13 days. These updates provided detailed analysis of the terrorist tactics, techniques, and procedures, and recommended protective measures based on the employed strategies. These updates, along with a Mumbai TRITON Special Report, were also shared with members of the private sector through postings on the HSIN-CS portal. TRITON reports are monthly or incident-reactive reports that assess terrorist tactics, techniques, operations, and strategies. TRITON reports are produced by a UK-based subject matter expert company, and are provided by IP to our State and local government TRIPwire users.

On December 1, IP e-mailed an updated TRIPwire SIR that contained additional information to all TRIPwire system users and the National Infrastructure Coordinating Center (NICC). IP also posted the SIR to the TRIPwire website "What's New" Portal and to HSIN-CS. Of note, during the eight-day timeframe of November 27 to December 4, TRIPwire had over three times the average number of site visits, indicating intense user interest in the Mumbai attacks and the terrorist tactics, techniques, and procedures used in the attacks.

On December 2, IP's Commercial Facilities SSA-EMO coordinated a conference call with over 200 leaders across all sectors. The Department's Office of Intelligence and Analysis (I&A), Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), IP, and Transportation Security Administration provided detailed information on the Mumbai attacks to call participants. Their briefings included analyses of the tactics, techniques, and procedures used in the Mumbai attack, and provided security recommendations to address these attack methods. Specific protective measures were proposed to address surveillance, target selection, infiltration, target access, and engagement with security forces. Based on positive feedback from that call, an additional conference call was held on December 10 specifically for 75 leaders of the Banking and Finance Sector.

On January 12, I&A and IP conducted a classified briefing for senior security directors representing major hotel chains and other commercial venues. The briefing provided a detailed analysis of the tactics, techniques and procedures used in the Mumbai attacks, including specific details of the IEDs; terrorist exploitation of technology; surveillance techniques; timeline of the attack including the targets and tactics; and recommended protective measures for surveillance, port security, access control, and coordination with security forces on specific actions to improve the security posture at their location.

In addition to the interactions with our NIPP partners in Washington, D.C., a significant portion of IP's work is conducted in the field, across the United States, by the Protective

Security Advisor (PSA) cadre. Eighty PSAs are in place in communities throughout the Nation to assist with State, local and private sector efforts to protect critical assets, providing a Federal resource to communities and businesses. During natural disasters and contingency events such as Mumbai, PSAs often work in State and local Emergency Operations Centers. PSAs also provide real-time information on facility significance and protective measures to facility owners and operators, as well as State and local representatives. For example, during the Mumbai event, the PSA for Las Vegas met with hotel, casino and resort security officials to answer questions and distribute our CV/PI/PM reports that provide details on enhanced security recommendations and best practices.

PSAs also conduct Enhanced Critical Infrastructure Protection (ECIP) assessment visits to assess overall site security, identify gaps, recommend protective measures, educate facility owners and operators on security, and promote communication and information sharing among facility owners and operators, DHS, and State governments. Information collected during ECIP visits will be used to develop ECIP metrics; conduct sector-by-sector and cross-sector vulnerability comparisons; identify security gaps and trends across CIKR sectors and sub-sectors; establish sector baseline security survey scores; and track progress toward improving CIKR security through activities, programs, outreach, and training. This information is utilized during incidents to help focus national and local response efforts on identified areas of criticality within the impact area and assist in the prioritization of reconstitution efforts.

In addition to the PSA program, IP has provided support for reducing risk of a terrorist attack to the Nation's CIKR by conducting vulnerability assessments for assets in the Commercial Facilities Sector. The Buffer Zone Protection Program (BZPP) is a DHS-administered grant program designed to help local law enforcement and owners and operators of CIKR increase security in the "buffer zone"—the area outside a facility that can be used by an adversary to conduct surveillance or launch an attack. The BZPP focuses on identifying and mitigating vulnerabilities at the highest-risk critical infrastructure sites and is designed to increase local law enforcement capabilities and preparedness.

Additional support is provided through Site Assistance Visits (SAVs). These are "inside the fence" vulnerability assessments conducted jointly by IP in coordination and cooperation with Federal, State, local, and CIKR owners and operators that identify critical components, specific vulnerabilities, and security enhancements. During an SAV, consequence and vulnerability information is collected to inform risk data, which is then used as supporting information for risk-based decision making.

IP has also conducted training for more than 1,900 stakeholders in the Commercial Facilities Sector and law enforcement officials who protect assets in the Lodging and Resorts Subsectors. Relevant courses include Soft Target Awareness, Surveillance Detection, IED Awareness, and Protective Measures.

To provide additional assistance to the Commercial Facilities Sector, IP is currently deploying Risk – Self-Assessment Tool (R-SAT), an upgraded, re-engineered version of the Vulnerability Identification Self-Assessment Tool (ViSAT). ViSAT is a Web-based self-assessment tool developed by IP and provided free of charge to CIKR asset owners/operators, primarily in places of mass gatherings such as arenas and stadiums. This tool assists owners/operators to raise the level of security at CIKR facilities and establish a common baseline of security from which all assets in certain sectors or subsectors can identify weaknesses and establish protection plans. Modules have currently been deployed for stadiums, arenas, convention centers, performing arts centers, and speedways. Commercial facilities members currently have access to ViSAT, and DHS has provided a grant to the International Association of Assembly Managers, a co-chair of the Public Assembly Subcouncil, to promote and provide training for this tool.

IP also provides the Constellation/Automated Critical Asset Management System (C/ACAMS) to State and local communities at no cost. Currently, 30 States use C/ACAMS, a CIKR asset management system that focuses on the unique requirements and information needs of first responders. It provides vulnerability and consequence scoring tools that aid the user's subjective analysis of criticality; an integrated open source information portal, Constellation, which ties together critical asset data and reporting about the current threat environment; a tailored reporting capability to assist in data calls on critical assets; Buffer Zone Generation capability; capability to generate pre-incident operational plans; online resources for first responders; and an integrated geographic information system via the Department's Integrated Common Analytical Viewer.

Additionally, the Regional Consortium Coordinating Council (RCCC) was established in Fall 2008 to bring the unique perspectives of geographically based public and private partnerships into the NIPP framework. The RCCC comprises existing functional and active regional entities that include both government and private sector members. The RCCC provides a critical link between CIKR owners/operators and key homeland security officials and activities at the regional, State, and local levels.

These Departmental efforts and resources are critically important. However, as we move forward and enhance our efforts, and recall the lessons learned from Mumbai, it is also important to acknowledge that individual facility owners and operators, and their State and local officials, know the unique circumstances facing a specific asset and are, therefore, best positioned to serve as primary lead in coordination of security and emergency response planning. DHS's role is to facilitate and augment planning and support where necessary and appropriate.

I believe a key opportunity to prevent the next attack in this country will be by local law enforcement and the private sector seeing something suspicious and taking action or calling that information into the proper authorities. Time and again, we have witnessed this effective solution both here in the United States during the Fort Dix and South Carolina incidents and overseas. The Federal Government and the Department of

Homeland Security can and do assist with these efforts by providing valuable information to our local government and private sector partners.

As I have described, IP is focused on continuing to improve our capability to provide timely and actionable information to our public and private sector partners. This, coupled with partnerships strengthened during recent hurricane experiences, has reinforced the operational linkages that will enable effective planning in advance of an incident, result in enhanced safety, security and resiliency of our nation's CIKR, and produce an operational effect for expeditious, efficient, and effective response should an incident occur.

Thank you for your attention, and I would be happy to answer any questions you may have at this time.