Statement for the Record

of

Charles E. Allen
Under Secretary for Intelligence and Analysis
U.S. Department of Homeland Security

Before the

Committee on Homeland Security and Governmental Affairs
United States Senate

January 8, 2009

Thank you, Chairman Lieberman, Senator Collins, and Members of the Committee for the invitation to discuss the lessons the Department of Homeland Security (DHS) learned following the recent terrorist attacks in Mumbai, India. I would like to highlight for you our intelligence information sharing efforts regarding these attacks.

The Office of Intelligence and Analysis routinely analyzes and provides information, in conjunction with the Federal Bureau of Investigation (FBI), on overseas terrorist threats and attacks with our state, local, tribal, and private sector partners to assist them in protecting our nation, its vital assets, and citizens. We have analyzed the November 26-30, 2008 Mumbai attacks, where members of a well-armed, and trained terrorist group made a maritime entry into the coastal city and then fanned out to attack multiple locations, including transportation, commercial, and religious facilities. The assailants apparently were familiar with target layouts and security postures, indicating pre-operational planning and surveillance. We continue to analyze the Mumbai attacks as new data become available, and we and the FBI will share this information broadly with our customers to help them protect our nation's citizens and critical infrastructure and to hone our capabilities to respond quickly and decisively to any terrorist attacks on the Homeland. Broadly, the lessons learned thus far can be categorized into prevention and deterrence, and response and recovery.

Prevention and Deterrence

We are reminded that disrupted plots may resurface. Indian authorities apparently arrested a Lashkar-e-Tayyba (LT) operative in February 2008 who carried with him information suggesting Mumbai landmarks, including the Taj Mahal Hotel, had been targeted for surveillance, possibly for a future terrorist operation. Indian authorities shared the information with the hotel owners and the security was bolstered at the Taj Mahal and at several other locations. Some time prior to the attacks, however, security at many of the sites identified in the February 2008 arrests was reduced to more routine levels. It is apparent now that LT's overall intention to attack Mumbai was not disrupted—LT plotters evidently had delayed their attack plans until a time of their choosing. This is a valuable lesson that we have also learned from the multiple plots planned against New York City, including the World Trade Center Towers, before the September 11 attacks brought the towers down. This lesson appeared to have been repeated in Mumbai. An intelligence informed threat warning and a heightened security posture may have delayed the attack in Mumbai, but LT plotters continued to plan for attacks on Mumbai's financial and entertainment center. DHS and the intelligence and law enforcement communities must remain cognizant that targets identified in previous plots are likely to resurface in the future.

A determined and innovative adversary will make great efforts to find security vulnerabilities and exploit them. The Mumbai attackers entered the city via the sea because they may have believed it was the best rout to avoid detection. Sea infiltration permitted the attackers to com ashore with a substantial cache of weapons that might have been detected during a land entry into the city. Terrorists are always seeking to identify weaknesses in our security and exploit them. Vulnerability assessments used to develop security and protective protocols must look closely at our nation's assets from

the perspective of the terrorist, vigorously seek the weaknesses that they can exploit, and work tirelessly to minimize if not eliminate those weaknesses.

Security must be unpredictable for the adversary, but predictably responsive to those it is meant to protect. The Mumbai attackers were able to ascertain the routines and vulnerabilities of the security forces at the primary targets during the pre-operational phase. For this reason, it is important to vary security routines and establish capabilities to "surge" security forces, such as we have done in DHS, through the Transportation Security Administration, with our Visual Intermodal Prevention and Response (VIPR) teams. In addition, during the period of heightened security, several of the hotels that were attacked installed security scanning devices. According to open source reporting, some of these devices were not in operation during the attacks, and all security personnel were not properly trained on those devices that did work. Effective training of private sector security personnel and first responders is an essential element of securing our nation's critical infrastructure—85 percent of which is privately owned. Training of the private sector on detection, deterrence, response and recovery is essential to protecting our homeland. To that aim, my office shares, on a routine basis, intelligence-derived threat information on potential adversaries and their tactics with state, local, and tribal authorities, and private sector security personnel. This information can be used to develop coordinated public-private response plans and train first responders on how best to respond to various attack methods that may be employed by terrorists so as to better protect personnel and resources.

Target knowledge was paramount to the effectiveness of the attack. The terrorists were able to collect sufficient information on all targets to execute a successful attack. Much of the information they required was accessible through open sources that are readily available in any open society. Hotels, restaurants, and train stations by their nature are susceptible to extensive surveillance activities that might not necessarily draw attention because the public is frequently moving through them. In the Mumbai attacks, during the planning and training stages, the cells reportedly used information from commercial imagery providers as well as pictures and videos from each of the targets acquired by support personnel. Surveillance by terrorist operatives or support personnel represents an opportunity to identify and interdict terrorist operatives. The Department is working, in cooperation with the Office of the Director of National Intelligence (ODNI), the Federal Bureau of Investigation (FBI), and our state, local, tribal, and private sector partners to establish a comprehensive Suspicious Activity Reporting system that is designed to systematically collect and identify possible pre-attack activity.

"Low tech" attacks can achieve terrorist strategic goals—and can be dramatically enhanced by technology enablers. The Mumbai attackers were able to locate precise landing points by using Global Positioning System (GPS) for navigation. The attackers also were able to fend off the Indian response force because they were heavily armed with automatic rifles and grenades—the weapons of a basic infantryman. The group reportedly received extensive training that may have included urban assault operations. In addition, the attackers used wireless communication devices, including satellite and cell phones, to coordinate movement activities, establish defensive positions, repel rescuers, and resist Indian efforts to suppress them. Open source reporting also indicates they monitored press coverage of the attack through wireless communication

devices—which may have been taken from hostages—that may have provided some tactical advantages against the Indian rescue forces.

Response and Recovery

Response to a similar terrorist attack in a major U.S. urban city would be complicated and difficult. The chaos the attacks created magnified the difficulty of mounting an appropriate response. First responders, in order to deal with such a crisis, must first and foremost have adequate information on what is occuring as well as the capability to mount a rapid and effective response that minimizes the impact of the attack. In Mumbai it was not immediately clear to authorities whether there were multiple attack groups or a single group. The attackers were able to exploit the initial confusion because of the indiscriminate firings to move on to new targets. While preparedness training for this type of attack may not have prevented it, the effects likely could have been mitigated and reduced if authorities had been prepared and had exercised responses to terrorist attacks across all levels of government. Within the United States, our national exercises incorporate not only federal interagency participants, but also include regional, state, and local authorities, in order to identify potential gaps in our responses.

A unified command system is of paramount importance if governments are to respond to terrorist attacks quickly and effectively. Within the United States, we have developed the National Response Framework (NRF) and the National Incident Management System (NIMS) that provide us with a unified command system to respond to such attacks as well as natural disasters. This framework, while not a panacea, does provide guidance on organizational roles and responsibilities during response and recovery operations. The NRF and NIMS also provide mechanisms to convey to the public critical information, such as areas to avoid during an incident or the potential for additional attacks in other areas or regions.

Public-private interactions are crucial and must be developed before an incident occurs. Developing these relationships before an incident helps facilitate the flow of information during the crisis and may help ensure the data conveyed to first responders are accurate, such as changes in floor plans or access routes. Within DHS, the Office of Infrastructure Protection manages many public-private partnerships. Our efforts to build bridges between intelligence analysts and the owners and operators of the private sector that operate most of our critical infrastructures is ongoing and sustained. Furthermore, there are also many programs in operation and under development at the state and local level to expand relationships between owners and operators and first responders.

Threat Information must be quickly and accurately conveyed to the public. Accurate information serves to protect the public, reassuring them that the government is responding appropriately to the threat or attack. Information flow must be timely and managed in a manner that prevents the terrorists from potentially benefiting from what the authorities know about the attackers. Within DHS, we have established procedures and protocols to release accurate threat information quickly. These procedures during an incident include a thorough review to ensure protection of sensitive information. We have exercised this process on numerous occasions.

Training exercises that integrate lessons learned are critical. Through various national and state programs, DHS and agencies with homeland security responsibilities have exercised and practiced our coordinated response to terrorist attacks. We have taken the lessons learned in the September 11 attacks and the many attacks that have occurred overseas, and incorporated them into our national planning exercises. We have practiced coordinating responses to multiple attacks across federal, state, local, and tribal authorities. We will incorporate Mumbai-style attacks in future exercises to refine further our response capabilities. We have identified shortfalls and gaps, such as interoperable communications systems and intelligence analytic capabilities at the local level, and are using the DHS grants programs to address those shortfalls.

Lastly, ***we must protect the attack sites to collect intelligence and evidence to identify the perpetrators***. In many instances, it may not be readily apparent which group is responsible. While the preservation of life is paramount, preservation of crime scenes is an important consideration to identify the attackers and hold them accountable. This requires training and experience to execute effectively.

Now, let me briefly convey the information sharing actions of my Office of Intelligence and Analysis (I&A)—in conjunction with our partners at the FBI—during and after the Mumbai attacks. You also asked that we discuss DHS' information sharing with India following the attack. I respectfully request that we leave discussions of what has specifically been shared for a closed session to protect information the Indian government deems sensitive. I will note, however, that we have been working very closely with the Indian government to provide any information and assistance that we can.

Information sharing with state, local, tribal, and private sector partners is central to the intelligence mission of I&A. As noted earlier, we share this information to better secure our nation's infrastructure and to protect its citizens, by ensuring state, local, and tribal authorities and private sector owners are aware of the threat environment and tactics that may be employed by would-be terrorists. In addition to distribution of unclassified analyses focused on the homeland security implications of the Mumbai attack, I&A staff also fielded numerous questions from state, local, and tribal authorities and our private sector partners.

— Less than 24 hours after the November 26th attacks, I&A, acting jointly with the FBI, released a situational awareness update with the most current, 'For Official Use Only' (FOUO), information. This product, titled *Islamic Militant Group Attacks Multiple Locations in Mumbai, India* was disseminated broadly to all federal, state, local, tribal, and private sector stakeholders.

— That same day, November 27, I&A analysts consolidated intelligence regarding the attack tactics and began drafting a report for federal, state, local, tribal, and private sector entities describing the attack and its implications for homeland security.

— Between November 28 and December 2, I&A analysts provided classified and unclassified briefings on the attacks to private sector organizations, including a teleconference with approximately 250 attendees from the Commercial Facilities Sector Coordinating Council (SCC), the Transportation SCC, the Electric Power SCC, the Partnership for Critical Infrastructure Security, the Federal Senior Leadership Council, the Information Sharing and Analysis Centers Council among others and the Homeland Security State and Local Community of Interest (HS-SLIC) State, Local, and Tribal, and Territorial Government Coordinating Council (SLTTGCC).

— On December 3, the FBI and I&A published a FOUO Joint Homeland Security Note, *Mumbai Attackers Used Commando-Style Assault Tactics,* describing our preliminary findings on the terrorist tactics used in Mumbai for federal, state, local, tribal, and private sector partners.

— I&A also released a FOUO background primer for federal, state, and local officials in early December on the LT terrorist organization. This "Homeland Security Reference Aid" discussed the group's history, leadership, membership, targeting preferences, and homeland nexus.

— In the weeks following the attacks, I&A has continued to provide classified and unclassified briefings, particularly to the private sector; tailoring presentations for the Nuclear SCC, the Financial Services Sector's SCC and Information Sharing & Analysis Center, and the Financial and Banking Information Infrastructure Committee.

Homeland security stakeholders have responded positively to our efforts and, according to I&A intelligence officers in fusion centers nationwide, their state and local counterparts have praised DHS for providing timely, relevant information in the attacks' aftermath. A senior security official at a large private company singled out I&A during a recent address, noting that the timely intelligence information provided by DHS was a "breath of fresh air."

I have touched on a broad range of information on the lessons learned and our information sharing activities in support of state, local, tribal, and private sector partners with information regarding the tragic attacks in Mumbai. DHS is making strong efforts to foster information sharing at all levels of government. We remain committed to implementing the information sharing mandates of the Intelligence Reform and Terrorism Act of 2004, the Homeland Security Act of 2002, and the August 2007 9/11 Commission Act. We do this with full concern for the civil rights, civil liberties, and privacy of all Americans.

Thank you and I look forward to your questions.