Statement by
Under Secretary Frank Libutti
Information Analysis and Infrastructure Protection Directorate
Department of Homeland Security
Before the House Financial Services Committee
August 23, 2004

Good morning Chairman Oxley, Congressman Frank and distinguished members of the Committee. I am pleased to appear before you today to discuss the protection of the financial services sector, including critical infrastructure protection initiatives. In my testimony today, I will provide an overview of the Information Analysis and Infrastructure Protection Directorate (IAIP), describe initiatives that the Department of Homeland Security has taken to protect the financial services critical infrastructure in general, and discuss some of the more specific actions taken after the recent elevation of the threat level to Code Orange for the financial services sector in New York City, Northern New Jersey, and Washington, DC.

Established by the Homeland Security Act of 2002, IAIP leads the Nation's efforts to protect our critical infrastructure from attack or disruption. The IAIP Directorate was created to analyze and integrate terrorist threat information, and to map those threats against vulnerabilities—both physical and cyber—to protect our critical infrastructure and key assets.

IAIP includes the Homeland Security Operations Center (HSOC), the Office of Information Analysis, the primary analytic center for threat information and intelligence within DHS, and the Office of Infrastructure Protection (IP). IP's mission is to lead the coordination of Federal, State, and local efforts to secure the Nation's infrastructure. I am responsible for all three.

In today's highly technical and digital world, we recognize that attacks against us may manifest themselves in many forms, including both physical and cyber attacks. In addition, we recognize the potential impacts one attack may have on a variety of other assets. This interconnected and interdependent nature of our infrastructure makes our physical and cyber assets difficult to separate, and it would be irresponsible to address them in isolation.

Recognizing the potentially devastating effects of disruption of services or catastrophic failures in the banking and financial sector, IAIP works on a daily basis to assess threats and vulnerabilities; mitigate risk; develop protective measures; and communicate with the sector. The banking and finance sector not only represents both physical and cyber vulnerabilities, but is also critically interconnected with every other critical sector within our Nation.

IAIP Coordination and Information Sharing

As directed by Homeland Security Presidential Directive 7, IAIP has focused on monitoring and assessing threats and vulnerabilities to all sectors, including the Banking and Finance sector. Sharing this information with the private sector is a vital component of IAIP's mission. DHS also acts as a coordinator with other government entities. In the financial field, IAIP partners with the US Treasury Department to share information with government entities and the private

sector through three entities: the Financial Services Sector Coordinating Council (FSSCC), a council of private-sector financial services associations, the Finance and Banking Information Infrastructure Committee (FBIIC), a body of government agencies, and the Financial Services Information Sharing and Analysis Center (FS-ISAC).

The FS-ISAC, established in 1999, provides a mechanism for gathering, analyzing, and appropriately sanitizing and disseminating information to and from infrastructure sectors and the Federal Government. Every two weeks the FS-ISAC conducts threat intelligence conference calls at the unclassified level for members, with DHS IAIP providing input. These calls cover physical and cyber threats, vulnerabilities, incidents that have occurred during the previous two weeks, and suggestions and guidance on future courses of action. The Financial Services ISAC, as with all ISACs, is capable of organizing crisis conference calls within an hour of the notification of a Crisis Alert. In addition, DHS has established close working relationships with the appropriately cleared senior members of the ISAC to exchange classified information as appropriate.

IAIP receives and evaluates current threat and incident information, including suspicious activity reports, submitted directly by the industry or through the ISAC and provides timely feedback on those issues. As recent events have exemplified, during times of elevated threat, IAIP intensifies its efforts to coordinate and reach out to the private sector, the entities described above and other government agencies.

IAIP Initiatives

In preparation for responding to threats and elevated threat levels, IAIP has been building and coordinating a two-way exchange of information with the public and private sectors. These efforts have also included building relationships with the private sector and government entities as well as implementing and integrating technical and information sharing solutions. I would like to take this opportunity to discuss two of these initiatives with you today.

HSIN-CI

The Homeland Security Information Network (HSIN) - Critical Infrastructure (CI) was launched earlier this summer and was specially designed to communicate real-time information to critical infrastructure owners and operators, 85 percent of whom are part of the private sector. HSIN–CI has the capacity to send alerts and notifications to the private sector at a rate of:

- 10,000 simultaneous outbound voice calls per minute
- 30,000 inbound simultaneous calls (hot line scenario)
- 3,000 outbound simultaneous faxes
- 5,000 outbound simultaneous Internet e-mail

The Homeland Security Operations Center (HSOC) regularly disseminates domestic terrorism-related information generated by the Information Analysis and Infrastructure Protection Directorate, known as “products” to Federal, State, and local governments, as well as private-sector organizations and international partners. The HSOC communicates in real-time to its

partners by utilizing HSIN internet-based counterterrorism communications tool, supplying information to all 50 states, Washington, D.C., and more than 50 major urban areas. Threat products come in two forms:

- Homeland Security Threat Advisories which are the result of information analysis and contain actionable information about an incident involving, or a threat targeting, critical national networks, infrastructures, or key assets. They often relay newly developed procedures that, when implemented, significantly improve security and protection. Advisories also often suggest a change in readiness posture, protective actions, or response, and

- Homeland Security Information Bulletins which are infrastructure protection products that communicate information of interest to the nation's critical infrastructures that do not meet the timeliness, specificity, or significance thresholds of Threat Advisories. Such information may include statistical reports, periodic summaries, incident response or reporting guidelines, common vulnerabilities and patches, and configuration standards or tools.

IAIP Response to Recent Financial Services Sector Threat

Before I address the role of IAIP in protecting our nation's critical financial infrastructure, I would be remiss, given this Committee's leadership in the fight against terrorist finance and financial crime, if I did not take a moment to highlight for you the other important role of DHS relative to the financial services industry – that is, our role in the investigation of a wide variety of financial crimes.

I know this Committee is uniquely positioned to appreciate the depth of financial investigative expertise and jurisdiction now housed within the Department of Homeland Security. The investigative functions and personnel of the former U.S. Customs Service, now housed within Immigration and Customs Enforcement, include some of the most experienced financial investigators in the U.S. government. In addition, DHS is also home to the United States Secret Service, which has, as one of its primary missions, the investigation of counterfeiting, credit card fraud, access device fraud, and cyber crime. Together, they represent a vast and impressive array of expertise critical to protecting our Nation's financial systems. ICE's investigative work in the areas of bulk cash smuggling, unlicensed money remitters, and other non traditional financial mechanisms, greatly enhances the U.S. government's ability to combat financial crime and detect and address vulnerabilities within the financial systems.

The latest series of events against the U.S. financial institutions was spurred by ongoing concerns over al-Qaida's interest in targeting U.S. critical infrastructure as well as recent intelligence revelations of detailed reconnaissance against several U.S. financial institutions. Based on the multiple reporting streams and the information contained in these reports, the Intelligence Community concluded that the information warranted the heightened alert status.

The level and specificity of information found was alarming, prompting DHS raise the threat level to ORANGE for the financial services sector in New York, northern New Jersey and Washington, D.C. on Sunday, August 1. This was the first time the level had been changed for an individual sector and geographic-specific area.

In response to the heightened threat level, IAIP acted on several fronts to address the threat. In accordance with established DHS notification protocol for raising the threat level, conference calls were arranged between DHS, FS-ISAC, FSSCC, FBIIC, state homeland security personnel, and local law enforcement. The Financial Services Roundtable, a private sector group representing the electronic commerce interests of the largest bank holding companies in the United States, was also included along with numerous other financial sector entities. In addition, senior leadership personally met with CEOs and Security Directors from the financial sector to better inform them of the evolving conditions and to provide guidance.

Simultaneously, Secretary Ridge activated the Interagency Incident Management Group to monitor and assess threat conditions. The IIMG is a headquarters-level multi-agency coordination entity that facilitates Federal domestic incident management activities. The mission of the IIMG is to provide strategic situational awareness, synthesize key intelligence and operational information, frame operational courses of action/policy recommendations, anticipate evolving requirements, and provide decision support to the Secretary of Homeland Security and other senior officials as requested during select periods of heightened alert and national-level domestic incidents. To accomplish this mission, the IIMG is task-organized to include representation from DHS components and staff offices as well as a tailored group of interagency participants.

Subsequent to providing immediate alerts to the financial sector regarding the threat, IAIP continued to work with the industry to ensure that all targeted financial institutions were individually briefed. IAIP coordinated with Federal, State, and local law enforcement entities to ensure that the appropriate information was exchanged between the government and the private sector. IAIP also polled the various financial institutions to determine what additional protective measures were implemented as a result of the heightened alert. This included the deployment of IAIP personnel to provide technical assistance to local law enforcement and facility owners and operators.

IAIP personnel were also immediately deployed to facilities in Washington, DC, New York City, and northern New Jersey. Teams of IAIP personnel conducted Site Assistance Visits (SAVs), in collaboration with local law enforcement officials and asset owners and operators, to facilitate vulnerability identification and discuss protective measure options. A total of 21 visits have been conducted thus far of facilities in the banking finance sector. Owners, operators, and security personnel were also given *Common Characteristics and Vulnerability* (CCV) reports and *Potential Indicators for Terrorist Attack* (PITA) reports to help them identify vulnerabilities and precursors to terrorist attacks.

In addition to SAVs, IAIP personnel have been working with individual facilities and local law enforcement entities to implement buffer zones around select banking and finance facilities. Buffer zones are community-based efforts focused on rapidly reducing vulnerabilities “outside

the fence" of select critical infrastructure and key resources. To support these efforts, IAIP provides assistance to local law enforcement officials to develop and implement buffer zones. To date, six buffer zone implementation plans for the banking and finance sector have been submitted to IAIP by State homeland security advisors.

Information gathered from SAVs and buffer zone implementation plans, and updates from the threat data, is being given to the Principal Federal Official (PFO) in New York City. The PFO is a US Secret Service agent designated by DHS as the lead Federal official to coordinate activities surrounding the Republican National Convention, a National Special Security Event (NSSE), and to coordinate department activities in response to the specific threat. IAIP personnel are assigned to the PFO staff to provide expert, subject-based knowledge and act as a conduit to resources held by the rest of the department. IAIP continues to support the New York PFO in the days leading up to the Republican National Convention with updated information, technical expertise, and material assistance when appropriate.

At this time, IAIP is continuing to work on assessing the threat posed by the recent surveillance discovery. IAIP is also studying the interdependencies between the financial sector and other critical infrastructures. The purpose of this analysis is to determine the level of potential interdependencies if any of the targeted institutions are attacked, as well as whether attacks on other critical infrastructure could even more seriously impact the financial sector. The results will be used to identify whether additional protective measures are required.

As I have discussed with you today, IAIP has taken many actions to secure the financial services sector. Our job, however, is not done. We will continue to monitor the evolving threat conditions and communicate even better with the private sector. Together with the Department of Treasury, we have laid the foundation for a true partnership with the public and private sector. Based on this foundation, and with continued dedication, we will continue to work to protect our Nation.

Again, thank you for the opportunity to testify before you today. I would be pleased to answer any questions you have at this time.