Statement by
Robert Liscouski
Assistant Secretary for Infrastructure Protection
U.S. Department of Homeland Security
Before the House Financial Services Committee
September 8, 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 some of the more specific actions the Department of Homeland Security (DHS) has 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 my office, 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.

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 it 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 and other government entities is a vital component of IAIP's mission.

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.

The Homeland Security Information Network (HSIN) - Critical Infrastructure (CI) was launched earlier this summer and was specially designed to communicate real-time information to owners and operators of critical infrastructure, 85 percent of which is owned by 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

In addition, the Homeland Security Operations Center (HSOC) regularly disseminates terrorism-related information generated by IAIP, 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.

- 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.

Sector Coordinating Councils and Sector Information Sharing

The Financial Services Sector has developed two effective mechanisms for the two-way sharing of information. The first is the Financial Services Sector Coordinating Council (FSSCC), which consists of senior representatives of major financial institutions representing a cross section of the financial industry. The FSSCC provides an orderly and effective venue for the financial sector and the Government to engage on the broad range of Homeland Security and critical infrastructure issues. In addition, the financial sector maintains the Financial Services Information Sharing and Analysis Center (FS-ISAC). The FS-ISAC was established in 1999 under the aegis of a Financial Services Steering Committee (now the Financial Services Sector Coordinating Council) representing the sector. It provides a mechanism for gathering, analyzing, and appropriately sanitizing and disseminating information to and from its members and the

Federal Government. Every two weeks the FS-ISAC conducts threat intelligence conference calls at the unclassified level for subscribed members, with 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.

Sector Coordinating Councils are emerging as a primary conduit for communication and coordination with the Federal government and many critical infrastructures and key resource industries. Private industry, on its own volition, organizes these forums to address national planning, common issues, develop best practices, and to find common solutions. Most sectors have established information sharing entities, such as Information Sharing and Analysis Centers (ISACs) to collect information on cyber and physical incidents and to disseminate alerts, warnings, and advisories to their members. At times, they also provide the communication vehicle for best practices and other security information tailored for each sector.

The Sector Coordinating Councils and their ISACs maintain and provide DHS with distribution lists which allow them to quickly disseminate threat warnings, alerts and advisories to members of their sectors. Information provided by the sectors is incorporated into the DHS situational awareness picture together with Intelligence Community and Law Enforcement information concerning possible threats to the nation's critical infrastructures. In addition, DHS has established close working relationships with the appropriately cleared senior sector members, including members from the financial services sector, 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 their information sharing entity, and provides timely feedback on those issues. As recent events have demonstrated, 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.

Protection of Critical Infrastructure

Terrorists are willing to exploit a wide range of infrastructure vulnerabilities. That is why we must continue to be vigilant and flexible in our approach to infrastructure protection.

Since the signing of Homeland Security Presidential Directive-7 in December 2003, IAIP has been engaged in numerous activities to protect our Nation’s critical infrastructure, including the development the National Infrastructure Protection Plan (NIPP), a key requirement of the Directive. The NIPP will delineate roles and responsibilities among the federal, state, local, and private sector stakeholders, establish national goals for critical infrastructure protection, and describe how DHS will lead the effort to integrate critical infrastructure protection activities across the sectors.

As a key part of the NIPP, the Sector-Specific Agencies designated in HSPD-7 are developing plans to identify critical infrastructure assets; identify and assess vulnerabilities and prioritize sector assets; develop protective programs; and measure the effectiveness of these programs. IAIP has worked closely with the Department of Treasury to develop the Banking and Finance sector plan.

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.

IAIP is working closely with the Science and Technology Directorate, other entities across the Department of Homeland Security, the Departments of Defense and Commerce, as well as the private sector to develop better methods for assessing the trustworthiness of cyber systems and the software which drives the financial services and other critical infrastructures of our nation. Software produced both domestically and offshore may have unintended flaws. Efforts are underway to work with the private sector to ascribe better measures of trustworthiness to software products and focus on achieving a number of common objectives. Such objectives include lowering development costs, reducing the time required to assess systems, and enhancing security protocols.

In addition, the Department of Homeland Security unveiled the National Cyber Alert System, an operational system developed to deliver targeted, timely, and actionable information to Americans to secure their computer systems. It is important to inform the public about the true nature of a given incident, what the facts are, and what steps they can and should take to address the problem. The National Cyber Alert System provides that kind of information. We have already issued several alerts and products in a periodic series of "best practices" and "how-to" guidance messages. We strive to make sure the information provided is understandable to all computer users, technical and non-technical, which reflects the broad usage of the Internet in today's society.

Working with IP, the United States Secret Service joined forces with the Carnegie Mellon University Software Engineering Institute's CERT® Coordination Center (CERT/CC), in order to conduct the Insider Threat Study. The study is a collaborative effort to better understand insider activities affecting information systems and data in critical infrastructure sectors, to include the banking and finance sector. This study is the first of its kind, and provides a comprehensive analysis of insider actions by analyzing both the behavioral and technical aspects of the activity.

The Insider Threat Study examines incidents when employees intentionally exceeded or misused an authorized level of system access that affected the organization's data, daily business operations, system security, or other areas via a computer. The study focuses on the on-line behaviors and communications that insiders engaged in before the incidents.

The goal of the study is to determine whether information may have been known or detectable prior to the incident; and to develop information to help private industry, government, and law enforcement better understand, detect, and ultimately prevent harmful insider activity.

On August 24, 2004, the first part of the report was released to the public sector; it is referred to as the Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector. This portion of the report focused on individuals who have had access to and have perpetrated harm using information systems in the banking and finance sector, which includes credit unions, banks, investment firms, credit bureaus, and financial institutions. The findings highlighted in this area of the report are of great benefit to the financial sector, as it provides concrete examples of how insiders accomplished their activities and offers suggestions on what security and/or policy procedures may have deterred or prevented such activity from occurring.

IAIP Response to Recent Intelligence Involving the Financial Services Sector

The IAIP response in the financial sector was spurred by concerns over al-Qaida's interest in targeting U.S. critical infrastructure as well as recent intelligence revealing 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 officials or entities. 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 (IIMG) 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. I AIP 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, was given to the Principal Federal Official (PFO) in New York City. IAIP personnel were 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 supported the New York PFO in the days leading up to and during 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 to determine the 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.

There are several lessons learned from this current change in threat alert level. As we have experienced in the past, early communications with the affected companies and local law enforcement help private sector security managers and law enforcement develop better coordinated and more effective responses. Prior Site Assist Visits conducted by DHS/IP/PSD at financial sector locations assisted PSD in its outreach to communicate the ORANGE threat level actions to mitigate the threat. Specific information had been shared with the private sector and local law enforcement on attack methods previously employed by terrorist groups and the specific actions needed to mitigate or disrupt potential attacks. This enabled the targeted locations to develop an early warning capability to begin crisis management procedures and implementation of additional appropriate protective measures. IP/PSD teams were deployed to the threatened sites and areas to assist the PFO, liaison with private sector and local law enforcement, and conduct gap analysis, advise on remediation methods and validate that the appropriate protective actions were undertaken.

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 the 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.