DEPARTMENT OF THE TREASURY
OFFICE OF PUBLIC AFFAIRS

EMBARGOED UNTIL 10:00 AM
September 8, 2004

Contact: Brookly McLaughlin
(202) 622-2960

Testimony of
Wayne A. Abernathy
Assistant Secretary of the Treasury for Financial Institutions
before the
Committee on Financial Services
United States House of Representatives

Wednesday, September 8, 2004

Introduction

Chairman Oxley and Ranking Member Frank, thank you for inviting me here today to testify on the progress of the financial services sector and the government in promoting the security and resilience of the nation's critical financial infrastructure.

I am pleased to tell you that the financial services sector is in an advanced state of readiness and preparation, and that it handled well the receipt of the recent information about terrorist targeting of specific financial institutions. No trading or financial activity was disrupted as a result of the recent threat elevation to Orange for the financial services firms in New York City, Northern New Jersey, and Washington, D.C. Customers were able to continue their business as usual. While there was concern, there was no crisis. There was no panic but rather activation of planned steps to mitigate exposure to risks. I congratulate the participants in the financial services sector for their actions, and especially for their excellent preparation, and I applaud our intelligence and law

enforcement agencies for obtaining this vital threat information and promptly sharing it with the affected institutions.

Organizing to Protect the Critical Financial Infrastructure

President Bush has led the development and implementation of an effective program to defend our country against terrorism. Protection of our financial infrastructure is a key element of that program, and much valuable work has already been done. That is because we have long known in general what recent information has reaffirmed with specificity, that our financial institutions are being targeted by our enemies.

The threat is not theoretical. Our nation's financial institutions are under assault virtually every day. Most of these assaults are in the nature of electronic or cyber attacks, such as computer viruses, Trojans, worms, and various forms of financial fraud, including phishing and spoofing. These assaults have progressed from computer hackers and pranksters, into theft, and now we believe on to schemes to disrupt the operations of our financial systems. Some of these attacks have their sources in organized crime. We believe that, increasingly, still more sinister actors are involved. I do not say this to be alarmist but rather to make the point that our financial institutions have for some time now been operating in a dangerous environment and are becoming increasingly adept at doing so successfully.

This success has not come easily, but as a result of careful organization and hard work on the part of the private sector and government agencies at all levels, federal, state, and local. The organized government effort is today based upon a directive from President Bush, Homeland Security Presidential Directive 7 (HSPD-7), which institutionalizes the national policy and overall framework for federal departments and agencies to identify, prioritize, and protect the critical infrastructure and key resources of our country. This is a flexible, coordinated program that works well in marshaling resources and activities in an organized fashion, agile enough to adjust to changed circumstances. HSPD- 7 places upon the Department of Homeland Security the central responsibility for coordinating the overall national program for critical infrastructure protection. While doing so, the Directive avoids reinventing the wheel, relying upon specific agencies to take the immediate lead—within the system of overall coordination by the Department of Homeland Security—thereby ensuring that critical protection efforts will continue to be led by departments that have the particular, sector-specific expertise and experience. The Department of the Treasury is the lead agency for the banking and finance sector and continues in that role under HSPD-7.

This arrangement has been tested several times in recent months and works well. I want to take a moment to commend Homeland Security Department Assistant Secretary Liscouski in particular for making this arrangement successful in practice, for ensuring that interagency cooperation has crowded out any opportunity for institutional rivalry. He has been and is a great partner, and we appreciate his efforts and those of the

dedicated men and women who work with him in the Information Analysis and Infrastructure Protection Directorate at DHS.

An important insight that informs the Administration's strategies is that nearly all of the financial critical infrastructure is owned by the private sector. As President Bush stated, "it is important to remember that protection of our critical infrastructures and key assets is a shared responsibility. Accordingly, the success of our protective efforts will require close cooperation between government and the private sector at all levels."

Not surprisingly, therefore, we work very closely with the private sector, and we do so on a cooperative, coordinated basis. This cooperation and coordination are made possible through reliance upon several private sector organizations. Chief among these is the Financial Services Sector Coordinating Council (FSSCC), the Chairman of which is the financial services Sector Coordinator, appointed by the Secretary of the Treasury. The current Sector Coordinator and Chairman of the FSSCC is Don Donahue, Chief Operating Officer of the Depository Trust and Clearing Corporation. The FSSCC is made up of entities and trade associations representing virtually every financial institution in the nation.

Alongside the FSSCC is the Financial Services Information Sharing and Analysis Center (FS-ISAC), an industry created and supported network that serves as the chief communications system for the financial services sector on a wide variety of threats and challenges to its members. Treasury has played an important role in significantly expanding the activities and membership of the FS-ISAC, so that it can meet the communication and coordination needs of financial firms of all sizes. Last year Treasury devoted $2 million to develop and implement a plan for restructuring the FS-ISAC, the results of which have been very encouraging. In the last couple of weeks, Federal Housing Finance Board Chairman Alicia Castañeda and I sent a joint letter to each of the Federal Home Loan Banks, encouraging them to join the FS-ISAC, and we continue our outreach efforts to encourage all financial firms to sign up.

Federal and state financial agencies are similarly organized and their activities coordinated to promote the security and resilience of the financial system. Under the sponsorship of the President's Working Group on Financial Markets, the Financial and Banking Information Infrastructure Committee (FBIIC) brings together all of the federal financial agencies as well as representatives of the state financial supervisors. Specifically, the FBIIC is chaired by myself, the Treasury Assistant Secretary for Financial Institutions, and includes representatives from the Commodity Futures Trading Commission, the Farm Credit Administration, the Federal Deposit Insurance Corporation, the Federal Housing Finance Board, the Federal Reserve Board (as well as the Federal Reserve Bank of New York), the National Credit Union Administration, the Office of the Comptroller of the Currency, the Office of Federal Housing Enterprise Oversight, the Office of Thrift Supervision, the Securities and Exchange Commission, and the Securities Investor Protection Corporation. In addition, state financial supervisors participate in the FBIIC through representatives from the Council of State Bank Supervisors, the North

American Securities Administrators Association, the National Association of Insurance Commissioners, and the National Association of State Credit Union Supervisors.

A cardinal rule of the FBIIC and a key to its success is the principal of responsibility. The FBIIC relies upon each agency to bear the full weight of its field of responsibility. The FBIIC does not try to take over that responsibility or interfere in the work of each agency in carrying out its statutory mandates. What the FBIIC provides is a means of coordinating those efforts, sharing best practices, pooling talents and resources, facilitating communication, encouraging wherever possible, cajoling when necessary. The Treasury Department has the role of orchestrating and facilitating this central service.

Some of the actions that Treasury has taken in recent months include the following:

- Arranging for critical financial institutions to have access to priority telecommunications services—both land-based and wireless—to help their voice and data communications get through during times of crisis.

- Assisting in coordinating the protective response of state and local authorities with critical financial institutions in their communities.

- Establishing systems and procedures that enable the federal financial regulators to communicate among themselves and with the private sector during times of crisis as well as in advance efforts to mitigate risks to the financial infrastructure.

- Conducting or sponsoring numerous tests, drills, and exercises to ensure that back up systems work and that financial professionals know what to do in times of either a heightened alert or an actual attack.

- Upgrading the Financial Services Information Sharing and Analysis Center (FS-ISAC) with financial assistance for new technology as well as for the development of a more inclusive business model that embraces all elements of the financial sector. This next-generation FS-ISAC now delivers integrated physical and cyber alert information to thousands of financial institutions and provides a secure, confidential platform to help financial institutions respond to potential or actual disruptions.

- Establishing a plan for working with the telecommunications, energy, information technology, and transportation sectors to address vulnerabilities introduced into the financial sector by interdependencies with these other sectors.

Recent Focused Elevation of the Threat Level

Our nation's enemies have shown themselves to be adaptive, innovative, and persistent. In the recent response to the threats against specific financial institutions we

have demonstrated that we have become even more adaptive, innovative, and persistent, ready to cope with a changing threat environment.

While the threats themselves are bad news, I see much good news in our latest experience. I am pleased to report that during the recent elevation of the threat level to code orange for New York City, Northern New Jersey, and Washington, D.C., the system created for promoting the security of our critical infrastructure has been working. Our anti-terrorism efforts are bearing fruit, providing valuable information, and that information is being applied and acted upon appropriately by the financial sector just as soon as it is made available, without disruption or degradation of services. This recent information was shared with the targeted institutions, with state and local governments, and with appropriate federal agencies. Treasury worked closely with DHS, coordinated activity within the FBIIC, and harmonized interaction with the FSSCC and through the FS-ISAC.

The response by the targeted financial institutions, and the financial sector as whole, was impressive. Action was immediate and business like. These institutions were able to use the information provided by the government to make informed decisions about the best course of action to take to protect their employees, customers, and the institutions themselves. They knew what to do because they had planned and prepared to address potential threats or disruptions. By and large, they implemented plans prepared well ahead of time.

Of course, the success does not lie in the plans themselves so much as with the people who developed and implemented them. I cannot say enough about the talent and dedication of the men and women of the financial services sector—in the private firms and in the public agencies. They deserve the thanks of those of us who use their services, and that includes just about all of us. Notwithstanding the threat information—that they had to view as alarming—these people energetically set to work to make sure that their protective measures and plans were implemented, and that the services they provide to their customers would continue without interruption. As I have said before this Committee and in outreach efforts around the country, our first priority is and must be people. And observing that priority works.

As a final point, in connection with the war on terrorism, the success of the collective actions of the federal, state, and local governments, and the preparedness and response of the private sector to promote the security and resilience of the financial sector, are progressively denying terrorists of their objective—their goal of disrupting our free markets. Freedom and free markets are the targets of the terrorists, and we are showing that we can harness the power of free people and free institutions to defeat the terrorists. There is much work yet to do, but tremendous work has already been done. Our markets are deeper, more resilient than ever before, and they are becoming more so every day.

This Congress and your Committee have been deeply interested and constantly supportive of this effort. Last year I reported to Chairwoman Kelly and the Oversight

Subcommittee on the financial sector's response to the power blackout. I had a good report to make then. I am pleased to report today that the financial sector continues to make progress, and we look forward to your continued interest, oversight, and support as we work on the tasks ahead.