Treasury's Ongoing Efforts as the Lead Agency for the Banking and Finance Sector Under PDD 63

OIG-CA-03-021 April 29, 2003

Office of Inspector General

****

The Department of the Treasury

Contents

Report 3

Background 4

Presidential Decision Directive 63 5

Principal Requirements 5

Other Requirements of PDD 63 8

The Banking and Finance Sector 10

The Department of the Treasury's Role as Lead Agency 14

The Formation of the Financial Services Information Sharing and Analysis Center (FS/ISAC) 15

The Formation of the Financial and Banking Information Infrastructure Committee (FBIIC) 16

Vulnerability Assessments 18

Education and Outreach, and Research and Development 19

Current Treasury Measures 22

GAO's Evaluation of Treasury's Performance as Lead Agency 23

Summary 24

Appendices

Appendix 1: Objective, Scope, and Methodology 26
Appendix 2: Major Contributors To This Report 27
Appendix 3: Report Distribution 28

Contents

Tables

Table 1: Lead Agencies for Sector Liaison 8
Table 2: Lead Agencies for Special Functions 9

Abbreviations

CIAO	Chief Infrastructure Assurance Officer
CIO	Chief Information Officer
Coordinating Committee	Banking and Finance Sector Coordinating Committee for Critical Infrastructure Protection
EO	Executive Order
FBIIC	Financial and Banking Information Infrastructure Committee
FEMA	Federal Emergency Management Agency
FFIEC	Federal Financial Institutions Examination Council
FS/ISAC	Financial Service Information Sharing and Analysis Center
FSSCC	Financial Services Sector Coordination Council
GAO	General Accounting Office
GETS	Government Emergency Telecommunications Service
ISAC	Information Sharing and Analysis Center
NCS	National Communications System
NIPC	National Infrastructure Protection Center
NS/EP	National Security and Emergency Preparedness
OIG	Office of Inspector General
PCCIP	President's Commission on Critical Infrastructure Protection
PCIPB	President's Critical Infrastructure Protection Board
PCIS	Partnership for Critical Infrastructure Security
PDD	Presidential Decision Directive
Treasury	Department of the Treasury
TSP	Telecommunications Service Priority Program
U.S.	United States

April 29, 2003

Michael A. Dawson
Deputy Assistant Secretary
Critical Infrastructure Protection and Compliance Policy

The Office of Inspector General (OIG) performed a limited review of the activities of the Department of the Treasury (Treasury) in its capacity as the lead agency for the Banking and Finance sector under Presidential Decision Directive (PDD) 63. Based on this review, we decided not to perform an audit of this area at this time. In making this decision, we considered the progress that Treasury and the industry have made, the extent of work recently performed by the U.S. General Accounting Office (GAO), and the current ongoing revisions in infrastructure protection strategy associated with the formation of the Department of Homeland Security effective March 1, 2003. We performed our review in accordance with the *Quality Standards for Inspections.*[1] We plan ongoing monitoring of this area, and will consider the need for an audit as we plan for Fiscal Year 2004 and future years.

We acknowledge that this is an area where there is ongoing activity, both within the industry and within Treasury, and where revisions continue to be made to address critical infrastructure issues. It should be noted, therefore, that this document contains information about activities through the end of our review, March 17, 2003. We have incorporated the informal comments that your office provided in response to our discussion draft of this report, as appropriate. This report provides general information about critical infrastructure issues and the status of Treasury in its

[1] The *Quality Standards for Inspections* were issued by the President's Council on Integrity and Efficiency during March 1993 and are available at www.ignet.gov/pcieecie, under *Quality Standards*.

role as lead agency for the Banking and Finance sector. It does not address Treasury's own internal critical infrastructure protection program.

Background

Technology has advanced at an explosive rate over the past years. The availability of computers has become a mainstay for the majority of today's workforce. Because of the nation's increased reliance on computers to perform daily functions, the need for increased security has also escalated. In response to the increased reliance on computers and the need to secure their information, President William J. Clinton signed Executive Order (EO) 13010 on July 15, 1996.[2]

EO 13010 stressed the importance of the national infrastructure[3] of the United States, emphasizing major sectors that were vital to the orderly continuation of services. It identified the following infrastructures as critical to the continued viability of the nation's defense or economic security: telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services, and continuity of government. The EO also established the President's Commission on Critical Infrastructure Protection (PCCIP), specified its mission, and identified its members and principal committees. Included in the PCCIP's overall tasks was an assessment of the scope and nature of the vulnerabilities[4] and threats to the nation's critical infrastructures.[5] The PCCIP was

[2] EO 13010 was subsequently amended by EO 13025 on November 13, 1996; EO 13041 on April 3, 1997; and EO 13064 on October 11, 1997.
[3] The national infrastructure is the framework of interdependent networks and systems comprising identifiable industries, institutions, and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the U.S., the smooth functioning of governments at all levels, and society as a whole.
[4] A vulnerability is a characteristic of a critical infrastructure's design, implementation, or operation that renders it susceptible to incapacitation or destruction by a threat.
[5] Critical infrastructures are those that are so vital that their incapacitation or destruction would have a debilitating impact on defense or economic security.

instructed to produce reports and recommendations to the Steering Committee as they became available.

The PCCIP completed and issued a report to the President titled *Critical Foundations: Protecting America's Infrastructures* on October 13, 1997. The report identified the vulnerabilities of the nation's critical infrastructures and offered recommendations to address these potential weaknesses. In addition to identifying the vulnerabilities of each of the sectors individually and the industry in its entirety, the report offers a strategy for actions that could be implemented to strengthen the areas where perceived weaknesses were identified.

Presidential Decision Directive 63

Principal Requirements

After the PCCIP report identified the susceptible areas of the nation's critical infrastructures, appropriate action was necessary. On May 22, 1998, President Clinton issued PDD 63, as his Administration's policy on critical infrastructure protection. PDD 63, which built on the information and recommendations in the 1997 PCCIP report, identified critical infrastructures as those physical and cyber-based systems essential to the minimum operations of the economy and government. The major sectors included, but were not limited to, the following industries:

- Telecommunications,
- Energy,
- Banking and finance,
- Transportation,
- Water systems, and
- Emergency services (both governmental and private).

PDD 63 specified that no later than 2000, the U.S. shall achieve an initial operating capability by significantly increasing security for government systems, and no later than 5 years from the day the President signed PDD 63, the U.S. shall achieve and be able to

maintain the ability to protect our nation's critical infrastructures from intentional acts that would significantly diminish the abilities of:

- The Federal government to perform essential national security missions and to ensure the general public health and safety;
- State and local governments to maintain order and to deliver minimum essential public services; and
- The private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial, and transportation services.

Most of the identified critical infrastructures reside in the private sector. Therefore, the responsibility for the protection of these critical assets rests mainly with private enterprises. Because of the enormity of this task, a coordinated effort between the private sector and the Federal government is required. In order to accomplish this task, PDD 63 appointed a lead agency for each critical infrastructure. PDD 63 further stated that the Federal government would appoint a senior officer from each designated agency as the Sector Liaison Official. Each Sector Liaison Official, after discussion and coordination with private sector entities of the applicable infrastructure sector, would identify a private sector counterpart, known as the Sector Coordinator, to represent the sector.

Together, these two individuals, one from the Federal government and one from industry, and the entities they represent, would contribute to a National Infrastructure Assurance plan by:

- Assessing the vulnerabilities of all of the sectors to cyber or physical threats,
- Recommending a plan to eliminate significant vulnerabilities,
- Proposing a system for identifying and preventing attempted major attacks,

- Developing a plan for alerting, containing, and rebuffing an attack in process and then, in coordination with the Federal Emergency Management Agency (FEMA)[6] as appropriate, rapidly reconstitute minimum essential capabilities in the aftermath of an attack.

Additionally, the lead agencies and their private sector counterparts would be responsible for developing and implementing a Vulnerability Awareness and Education Program for their sectors. Each Sector Liaison Official would collaborate with private sector representatives in addressing problems relating to critical infrastructure protection and would recommend components for the National Infrastructure Plan. Each Sector Coordinator, in consort with his or her private sector counterparts, would also be encouraged to create a private sector Information Sharing and Analysis Center (ISAC). The design and function of each center and its relation to the National Infrastructure Protection Center (NIPC)[7] would be determined by the private sector in consultation with the Federal government. Each center would serve as a mechanism for gathering, analyzing, appropriately sanitizing, and disseminating private sector information to both industry and the NIPC. Each center would also gather information from the NIPC for distribution to the private sector. The lead agencies and their corresponding critical infrastructure sectors are shown in Table 1.

[6] FEMA became part of the Department of Homeland Security's Division for Emergency Preparedness and Response as of March 1, 2003.

[7] The NIPC was instructed to serve as a national critical infrastructure threat assessment, warning, vulnerability, and law investigation and response entity. The NIPC includes members from the Federal Bureau of Investigation, the U.S. Secret Service, and representatives detailed from the Department of Defense, the Intelligence Community, and lead agencies.

Table 1: Lead Agencies for Sector Liaison

Lead Agency[8]	Critical Industry Sectors
Department of Commerce	Information and communications
Department of Energy	Electric power; oil and gas production and storage
Department of the Treasury	Banking and finance
Department of Transportation	Aviation, highways, mass transit, pipelines, rail, and waterborne commerce
Environmental Protection Agency	Water supply
Department of Justice/Federal Bureau of Investigations	Emergency law enforcement services
Federal Emergency Management Agency	Emergency fire service, continuity of government services
Department of Health and Human Services	Public health services, including prevention, surveillance, laboratory services, and personal health services

Source: White Paper – The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, May 22, 1998

Other Requirements of PDD 63

In addition to the specifics relating to the areas considered critical infrastructures, PDD 63 also detailed other requirements. There are several specific functions related to critical infrastructure protection that must be performed chiefly by the Federal government. Included under this designation are activities relating to national defense, foreign affairs, intelligence, and law

[8] It should be noted that some of the lead agencies, either in their entirety or in part, were transferred to the Department of Homeland Security effective March 1, 2003. Their responsibility for the critical industry sectors continues to exist.

enforcement. PDD 63 states that a lead agency would be responsible for coordinating the activities of the Federal government in these areas. Each lead agency would also be responsible for appointing a private sector Functional Coordinator for each function. Table 2 shows the lead agency for each of the four special functions.

Table 2: Lead Agencies for Special Functions

Lead Agency	Special Functions
Department of Defense	National defense
Department of State	Foreign affairs
Central Intelligence Agency	Foreign intelligence
Department of Justice/Federal Bureau of Investigation	Law enforcement and internal security

Source: White Paper – The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, May 22, 1998.

Also, a Critical Infrastructure Coordination Group chaired by the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism, would be formed to coordinate the implementation of PDD 63. This Group would consist of the Sector Liaison Officials, the Functional Coordinators, and representatives from other relevant entities, including the National Economic Council.

Additionally, a National Infrastructure Assurance Council would be established and staffed by appointees named by the President, based on the recommendation of the Lead Agencies, the National Economic Council, and the National Coordinator. The appointees would consist of a panel of major infrastructure providers and state and local government officials. The council would meet periodically to enhance the partnership of the public and private sectors in protecting the nation's critical infrastructures. Reports would be presented to the President as appropriate.

Lastly, each Federal government department and agency was directed to reduce its own exposure to threats against its own critical infrastructure. This requirement included the cyber-based systems. Every department and agency was to appoint a Chief Information Officer (CIO) who would be responsible for information assurance. Each department and agency was also to appoint a Chief Infrastructure Assurance Officer (CIAO)[9] who would be responsible for the protection of all other aspects of its critical infrastructure. The individual(s) were to establish procedures for obtaining expedient and valid authorizations to permit vulnerability assessments to be performed on government computer and physical systems.[10]

Each department/agency was also required to prepare a plan for protecting its critical infrastructure, including its cyber-based systems. Each plan was to be implemented within 180 days from the issuance of PDD 63, and to be updated every 2 years. The initial plan, a report with estimated completion dates for accomplishing the tasks associated with critical infrastructure protection, subsequent updates, and an annual report on the implementation of this directive was to be presented to the President and the heads of departments and agencies, through the Assistant to the President for National Security Affairs.

The Banking and Finance Sector

The Banking and Finance sector was identified in EO 13010, in the PCCIP's Report, and in PDD 63 as one of the nation's critical infrastructures. As noted in Table 1, PDD 63 appointed Treasury as the lead agency for this sector. Treasury's Assistant Secretary

[9] At the discretion of each department or agency, the CIO and CIAO may be the same individual.

[10] As mentioned previously, this review did not include an analysis of Treasury's role in this capacity. For additional information on Treasury's compliance with this aspect of PDD 63, refer to the following Treasury OIG audit reports: *Review of Treasury's Critical Infrastructure Protection Program*, OIG-01-025, issued on December 14, 2000, and *General Management: Treasury's Critical Physical Infrastructure Protection Program Needs Improved Guidance and Coordination*, OIG-02-024, issued on December 19, 2001.

for Financial Institutions coordinates critical infrastructure protection efforts between the Federal government and the sector.

The financial services sector[11] includes various specialized service organizations, such as the securities and commodities exchanges, funds transfer networks, payments networks, clearing companies, trust and custody firms, depositories, and messaging systems. In addition to those organizations that clearly belong in this group, there are additional firms that have become an indispensable part of the banking and financial services infrastructure. All of the aforementioned financial services entities have become increasingly reliant upon outsourcing certain activities to third party providers of systems and applications software in addition to acquiring third party technical expertise. These third-party firms have now become an integral part of the financial services industry.

A review of the banking and financial industry's history indicates that this sector is better prepared to address the potential threats to cyber and other infrastructure attacks. This preparedness is partially attributable to the reliance that the public places on these institutions. The maintenance of public confidence has been and continues to be of paramount importance in the financial services industry. Additionally, Federal regulators have required that entities such as financial institutions and securities brokers and dealers maintain a standard of security and emergency preparedness in order to safeguard their assets against potential losses, external as well as internal.

However, due to the constantly changing environment facing this sector, the industry must adapt and evolve its services and protections in response. Each new adaptation may result in new and varying vulnerabilities, which could have an adverse impact on various segments of the industry or on the industry as a whole. Therefore, the financial services sector must keep a constant vigil to the new changes to ensure that its infrastructures are modified as necessary. Some of the more common trends in the industry

[11] *Financial services sector* and *banking and finance sector* are used interchangeably in critical infrastructure documents.

and their potential effects on the sector's critical infrastructure include the following:

- Consolidation efforts in the financial services sector have resulted in a greater concentration of assets in a reduced number of financial intermediaries. If any of these individual entities experience any financial reverses, this could have a ripple effect throughout the financial industries sector by adversely affecting the smaller entities. Also, business enterprises are constantly faced with the challenge of reducing expenses to increase profitability. Coupled with the consolidation of industry members and the use of off-the-shelf software products, the surge to reduce overhead costs may create hostility with employees, especially with employees who get displaced because of any merger activities. An increased threat of insider vulnerabilities may result.

- Many entities have expanded their interests beyond the physical structure of their corporate headquarters and branch businesses. This expansion includes the use of card-activated terminals, wired and cellular devices, and personal computers. In keeping with the technological advancements, the business sector has replaced limited access computer systems with decentralized, open-access systems. Additionally, many businesses have adopted the use of shared networks. By completing business transactions on a shared network, rather than a dedicated network, the entities may increase their risk of unwanted intrusions. Financial transactions are no longer limited to the "9 to 5" banking hours. Transactions are occurring 24 hours a day, 7 days a week, in the financial markets on an international basis. The internet transmission of transactions permits individuals, corporations, and nations to conduct business at any moment and in any place. The ability to transact business ubiquitously may further increase vulnerabilities on a global scale. Each of these avenues can increase

the risk of unauthorized access by dissatisfied employees, computer hackers, or other unauthorized sources.

- Many businesses are increasing their reliance on external providers of services. For example, many financial institutions depend on third party servicers to provide data processing, system, and application functions. The interconnectivity between business entities and other industry sectors, such as telecommunications and energy, also presents potential risks. Any denial of service from an external provider may increase the vulnerability in the financial services sector.

On May 13, 2002, the Banking and Finance Sector submitted its input to the Partnership for Critical Infrastructure Security for *The National Strategy to Secure Cyberspace – Draft for Comment* report. This segment, titled *Banking and Finance Sector: The National Strategy for Critical Infrastructure Assurance*, Version 1.0, is a comprehensive document that details the sector composition, the industry's ongoing efforts, potential threats to the sector, strategic directions, enhanced foundation building, and considerations such as legal, regulatory, and law enforcement; insurance risk management; international aspects of critical infrastructure assurance; and interdependencies and collateral risks.

The *Banking and Finance Sector* segment includes appendixes containing information relating to the vulnerability assessment plan, research and development programs, education and outreach options and activities, and pending legislation. It focuses on the potential for disruption of services, the process for sector intervention and communication, and the reconstitution of services. It specifies how the owners and operators of the core infrastructure will respond in case of a catastrophic event and the government's assistance to the industry to prepare for such an event. Specific attention is devoted to an assessment and understanding of strengths and vulnerabilities; preparation, prevention, and recovery in the face of systemic attacks; detection and response to attacks on the information infrastructure;

reconstitution and restoration of technological and financial services and functions to their normal course of operations; and financial risk management in order to withstand the impact of attacks.

In order to reduce the threat of attacks in the financial services industry, Treasury is working in conjunction with members of the financial services sector to reduce or eliminate vulnerabilities faced by the financial services group through a partnership with the private sector.

The Department of the Treasury's Role as Lead Agency

As a result of the recommendations issued by the 1997 PCCIP and the requirements of PDD 63, Treasury was named as the lead governmental agency for the critical infrastructures of the financial services sector. The PCCIP's report, *Critical Foundations: Protecting America's Infrastructures*, precipitated the foundation of a coordinating committee known as the Banking and Finance Committee for Critical Infrastructure Protection (Coordinating Committee). This committee, which was a partnership of the public and private sectors, identified various goals that should be addressed, including (1) the dissemination of information within the private financial services sector, (2) assessments of the industry's vulnerabilities, (3) education and outreach, and (4) research and development. To accomplish these objectives, four corresponding working groups of individuals from the private sector were formed. The dissemination of information and the vulnerability assessments were considered to be the most crucial to the continued viability of the financial services sector. Actions taken for the two most crucial areas are discussed in detail below. Highlights of the education and outreach and of the research and development efforts are also included.

The Formation of the Financial Services Information Sharing and Analysis Center (FS/ISAC)

In 1999, the Coordinating Committee began using informal methods of transmitting information between the various participants within the Banking and Finance sector. Since the dissemination of information was limited to information sharing between "friends"[12] in the industry, information was not uniformly dispersed. This resulted in some entities gaining knowledge of potential problems and other entities remaining unaware that the problems existed or posed a possible threat.

The FS/ISAC, which became fully operational on October 1, 1999, was created to correct the disparate distribution of vital information within the financial services industry. The FS/ISAC is structured as a member-owned limited liability corporation, with membership required[13] for access. The composition of the group spans various branches of the financial services sector, including financial institutions, the insurance industry, brokerage firms, and utilities. As information is sent to the center from sources, which may choose to remain anonymous,[14] the analysts review the information,[15] sanitize it to avoid identification of the sender, and distribute the information to FS/ISAC members according to an alert priority. Reportedly, the current membership of the FS/ISAC controls 80-90 percent of the country's assets. To fulfill its role as the lead agency, Treasury participates in the activities of the FS/ISAC. Since the FS/ISAC is a private organization, Treasury is not involved with voting on issues presented to the group. However, Treasury remains an active participant in the FS/ISAC

[12] The term "friends" relates to individuals or entities that have an informal working relationship with others within the industry.
[13] Membership fees that ranged from $13,000 to $125,000, depending on the membership level selected, have been reduced to $7,000 per year for basic services.
[14] Anonymity is a hallmark for the FS/ISAC. Generally, the sources of information are FS/ISAC members. By maintaining anonymity, the various institutions are safeguarded from liability associated with sharing vulnerability information.
[15] The FS/ISAC contracted with Predictive Systems to review and analyze the information received by the ISAC.

meetings and offers advice on general topics or critical infrastructure issues when it is solicited.

Ideally, the Federal government would prefer that the financial services sector be notified by the FS/ISAC in the event of a cyber incident, rather than have information disseminated by other sources. Since the FS/ISAC knows the architecture of the systems, it is better equipped to distribute alerts in a proper context for this sector.

The Federal Financial Institutions Examination Council (FFIEC)[16] is compiling emergency protocol guidance to determine how the various regulators would respond and communicate in the event of an emergency. In determining how the various regulatory agencies would communicate with each other, the Financial and Banking Information Infrastructure Committee (FBIIC) decided that its members would communicate with the Homeland Security coordination center through one FBIIC representative. The response system was scheduled to be tested prior to the September 11 anniversary. However, it was put to the test as early as April 2002 when a bomb threat was made against the national banks in the Washington, D.C., area. The communications protocol has been tested on several occasions, and testing has also been completed on the secure phone and fax lines that were installed in each Federal agency. Conference calls using Government Emergency Telecommunications Service (GETS) cards have entered the initial testing phases. To date, all of the tests and uses of the communication system have been considered successful by Treasury.

The Formation of the Financial and Banking Information Infrastructure Committee (FBIIC)

On October 16, 2001, EO 13231 established the President's Critical Infrastructure Protection Board (PCIPB). One of the standing committees created as a result of the EO was the FBIIC,

[16] The FFIEC coordinates the regulatory guidance with the various primary Federal financial institution regulators.

which is chaired by the Treasury's Assistant Secretary for Financial Institutions. FBIIC members include, but are not limited to, the following: all of the Federal financial institution regulators, the Conference of State Bank Supervisors, the National Association of Insurance Commissioners, and the Securities and Exchange Commission. Initiatives established by the FBIIC include critical asset identification and vulnerability assessment, continuity of operations planning, and information dissemination. The FBIIC has working groups covering the following areas: vulnerability assessment, communications, international affairs, and legislative affairs.

In addition to the aforementioned efforts, other avenues have been developed to improve the industry's ability to communicate during emergencies. The Telecommunications Service Priority (TSP) Program permits certain financial institutions and other financial services to get priority restoration[17] for circuits. The TSP Program is administered by the National Communications System (NCS) and was developed to ensure priority treatment for the most important telecommunication services, which are those supporting National Security and Emergency Preparedness (NS/EP) missions. These telecommunications services are available to private sector entities through sponsorship by an NCS member department or agency. All non-Federal TSP requests must be sponsored by a Federal agency. FBIIC has developed policies and procedures on the sponsorship of priority telecommunications access for private sector entities. The TSP program authorizes and requires service vendors to provide and restore[18] TSP assigned services before non-TSP services and provides vendors with legal protection for giving preferential treatment to NS/EP users over non-NS/EP users.

Additionally, FBIIC has established a policy and application process for ensuring priority telephone communications among Federal agencies and essential financial service institutions during a period

[17] Financial institutions' priority is secondary only to emergency response organizations.

[18] A provisioning priority is obtained to facilitate priority installation of new telecommunication services. A restoration priority is applied to new or existing telecommunication services to ensure their restoration before any non-TSP services.

of national or regional emergency. This priority landline calling card system is known as GETS, and is designed to help assure communication between key public and private sector personnel during times of crisis. Financial institutions that are seeking sponsorship must complete an application and submit it to their primary Federal regulator. GETS allows calls to be placed in priority based on the access code on the calling card. Currently, wireless communication systems are being developed for high-priority calling services. They are not currently available for public access; however, it is possible that the use of satellite communication devices may be available to achieve the same results.

Vulnerability Assessments

In 1997, a contractor conducted a vulnerability assessment on the financial services sector. As mentioned, EO13231 established the PCIPB in October 2001.[19] Due to the numerous changes that transpired in the financial services sector during those intervening years (1997 until 2001),[20] the PCIPB requested a revised assessment. EO 13231 also created ten standing committees,[21] with one dedicated to the financial services sector. Treasury led the committee with the various regulatory agencies and other governmental entities serving as members. They focused their efforts on coordinating the Federal government's response to attacks. The various working groups, such as banking and finance, insurance, information technology and telecommunications, chemicals, oil and gas, electric power, law enforcement, higher education, transportation (rail), and water systems were involved

[19] The EO also established the FBIIC. EO 13286, dated February 28, 2003, amended EO 13231 as well as several other EOs and actions in connection with the transfer of certain functions to the Secretary of the Department of Homeland Security. The PCIPB established by EO 13231 was not included in the amended EO.

[20] Numerous banks were consolidating during this period, resulting in a concentration of large institutions. It was noted that several large banks were completing a greater percentage of the total dollar transactions.

[21] An eleventh committee is included in the EO, but it is not specified as belonging to a particular organization and is earmarked as "other."

with preparing reports for incorporation into the national infrastructure strategy.

On September 18, 2002, the PCIPB issued a draft of *The National Strategy to Secure Cyberspace*, with a 60-day comment period. The final strategy was released on February 14, 2003, as *The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets.* Barring any unusual circumstances that may require more frequent reviews, this strategy will be updated every 2 years. Additionally, other agencies and departments became involved in conducting assessments of the financial services sector.

The events of September 11, 2001, also triggered an immediate response in the financial services sector. It was discovered that secure telephone or fax lines did not exist within the various departments or agencies. Treasury provided secure telephones and fax machines for each of the Federal regulatory agencies. Treasury is in the process of establishing secured telephone and fax lines to state organizations such as the National Association of Insurance Commissioners, the Conference of State Bank Supervisors and new FBIIC members – the Federal Housing Finance Board and the Office of Federal Housing Enterprise Oversight.

Education and Outreach, and Research and Development

An effective education and outreach program is a necessary component for the financial services sector. Both the private and the public sectors have initiated various efforts in this respect. During the drafting of the *National Strategy to Secure Cyberspace*, the Partnership for Critical Infrastructure (PCIS)[22] played a vital role in facilitating the private sector's input to this strategy. Each critical sector, including the financial services sector, furnished a developing plan, which included initiatives that the sectors would

[22] PCIS is a public-private partnership that is also a non-profit organization administered by companies and private sector associations representing each of the critical infrastructure industries. The Critical Infrastructure Assurance Office provides support for the Partnership and government officials are invited to participate in meetings on a collaborative basis.

undertake in order to safeguard their applicable industry. The financial services sector plan stated that the goal of the education and outreach program was to build a sound foundation for the sector's critical infrastructure mission and initiatives among the key financial services system stakeholders. Financial sector actions geared toward infrastructure owners and operators include the following:

- Continue to support Treasury's hosting of annual meetings and conferences;
- Develop and communicate sound critical infrastructure assurance practices;
- Work with the Secretary of the Treasury to host an event for industry executives in conjunction with senior government and/or regulatory officials; and
- Continue briefings between industry associations and banking and finance senior executives on pertinent issues.

Financial sector actions directed toward public-sector officials include the following:

- Conduct briefings for public-sector officials, including Federal agencies and organizations, Congressional members and staff, state organizations and associations, and trade associations;
- Develop a list of action items that each target audience can undertake to assist in fulfilling the critical infrastructure protection;
- Develop uniform presentation materials and briefing documents; and
- Develop a list of sector executives who would accept referrals for speaking engagements.

The Financial Services Sector Coordinating Council (FSSCC)[23] is also undertaking an education and outreach effort. The FSSCC developed a working group to organize events related to homeland security and critical infrastructure protection.

The National Infrastructure Protection Center (NIPC) routinely sends bulletins to apprise the industry of events that are transpiring regarding the protection of critical infrastructures.[24] The bulletins are available on the NIPC website. The NIPC is an interagency center, which was initially established within the Federal Bureau of Investigation (FBI) and as of March 1, 2003, transitioned to the Department of Homeland Security. Treasury is developing an outreach communications plan, and it has been an active participant in speaking engagements to various interest groups to inform them of measures undertaken to safeguard the nation's financial services sector.

A contractor conducted a study of research and development (R&D) protocols in the market. Similar efforts were made for education and outreach. R&D issues have recently become a priority for Treasury, which is considering methods to fund efforts in this area. Treasury is currently undertaking a project to identify and stratify financial institutions based on their criticality to the industry. These institutions will be identified and segregated in tiers depending on their status in the financial services sector. The most critical financial services organizations have been identified, their vulnerabilities have been assessed, and work is under way to ameliorate their vulnerabilities. As each tier of critical institutions

[23] The FSSCC is a private sector initiative of the financial services industry, working in partnership with the government, to strengthen critical infrastructure protection initiatives to protect the U.S. financial sector and economy from attack.

[24] Additionally, the NIPC produces three levels of infrastructure warnings, which are developed and distributed consistent with the FBI's National Threat Warning System. The three levels consist of assessments, advisories, and alerts. An assessment addresses broad, general incident or issue awareness information and analysis that is significant and current but does not necessarily necessitate immediate action. An advisory addresses significant threat or incident information that suggests a change in readiness posture, protective option, and/or response. An alert addresses major threat or incident information addressing imminent or in-progress attacks targeting specific national networks or critical infrastructures.

is evaluated, other institutions will be segregated into their various tier groups according to perceived risks.

Current Treasury Measures

The terrorist attacks that occurred on September 11, 2001, have increased the focus on security in general, and, more specifically, on safeguarding the nation's critical infrastructures. After that date, Treasury established an Office of Critical Infrastructure Protection and Compliance Policy, which plays a key role in coordinating public and private efforts to protect the critical infrastructure of the financial services industry from attack. Among other duties, this Office staffs the FBIIC, discussed in the preceding sections. On February 4, 2003, Treasury announced the newly-created position of Deputy Assistant Secretary for Critical Infrastructure Protection and Compliance Policy as part of the Administration's ongoing effort to strengthen the nation's safeguards against terrorist activities and financial crime.

On March 17, 2003, President George W. Bush announced that the diplomatic deadline with Iraq elapsed without remedy. He issued an ultimatum to Iraq's leader and his offspring to either leave the country within 48 hours or face the threat of armed conflict. As the President was delivering his address, the U.S. Government raised the terror alert level to orange or "high risk." The Homeland Security Department announced Operation Liberty Shield, which includes increased security measures at ports of entry and in the airspace surrounding Washington, D.C., and New York City. In response to these announcements, Treasury's Office of Public Affairs issued a press release on March 17, 2003, announcing the issuance of a circular titled *Treasury Statement on Measures to Protect the Financial Markets During Hostilities with Iraq*. The fact sheet presents steps that have been taken to protect the critical financial infrastructures by Treasury, the Federal financial regulators, and the critical financial institutions.

GAO's Evaluation of Treasury's Performance as Lead Agency

GAO recently issued three reports and presented Congressional testimony related to PDD 63 efforts in the financial services sector. In a January 2003 report,[25] GAO recommends that Treasury coordinate with the industry (1) in its efforts to update the sector's *National Strategy for Critical Infrastructure Assurance* and (2) in establishing interim objectives, detailed tasks, time frames, and responsibilities for implementing it and a process for monitoring progress. With reference to the second point, the report states that Treasury should assess the need for grants, tax incentives, regulation, or other public policy tools to assist the industry in meeting its goals.

This GAO report also enumerates the various efforts that Treasury has taken to fulfill its role under PDD 63. For example, the report acknowledges that Treasury has taken steps designed to establish better relationships and methods of communication between regulators, assess vulnerabilities, and improve communications with the financial services sector.

[25] This report is titled *Critical Infrastructure Protection: Efforts of the Financial Services Sector to Address Cyber Threats* (GAO-03-173, January 2003). The other two GAO reports, which are based on a study of the events of September 11, 2001, contained recommendations only for the SEC. These reports, both titled *Potential Terrorist Attacks: Additional Actions Needed to Better Prepare Critical Financial Market Participants*, were issued February 12, 2003, as GAO-03-251 to the study's Congressional requesters, and as GAO-03-414 to the Committee on Financial Services, House of Representatives. On the same date, GAO's Director of Financial Markets and Community Investment presented testimony titled *Potential Terrorist Attacks: More Actions Needed to Better Prepare Critical Financial Market,* GAO-03-468T. In addition, GAO highlighted the issue of critical infrastructure protection in its *High-Risk Series* report titled *Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures*, GAO-03-121, issued during January 2003. Copies of these reports are available under the *GAO Reports* section at www.gao.gov.

Summary

Our evaluation of Treasury's mandate to serve as the lead agency for the financial services sector governing the physical and cyber security of the industry has been, and continues to be, an ongoing effort. To successfully complete all of the tasks enumerated under PDD 63 will require extensive time and effort on the part of the private sector, Treasury, and the affiliated organizations that have been developed as a result of the directive. To date, Treasury and the private sector have made advancements in establishing a separate information sharing entity to collect, analyze, and disseminate crucial information pertaining to potential threats to its members in a timely manner. Additionally, communication channels are open and operating between the private and public sectors, which enables both segments to articulate any perceived threats or problems that may or could exist. Also, several deficiencies that were highlighted following the September 11th events, such as unsecured telephone lines, have been eliminated.

The question as to whether or not the actions of Treasury and the private sector will enable the financial services sector to align and operate if another event such as September 11th occurs still remains. Even though testing of various component parts has been conducted, it is not possible to state with any degree of certainty whether a catastrophic event would have an adverse impact on the financial markets to operate, because testing of the entire system under simulated circumstances of this magnitude cannot be conducted. However, efforts by Treasury and the private sector to date would indicate that the financial services sector would have the ability to operate in the aftermath of an attack. The deadline for compliance with PDD 63 is May 2003. Although total compliance with the directive may not be achieved, Treasury is making a concerted effort to fulfill its obligation in its capacity as the lead agency for Banking and Finance.

Our office will continue to monitor Treasury's efforts as the lead agency for the Banking and Finance sector, including actions taken

in response to GAO's recommendations in its January 2003 report. We will initiate further reviews or audits as deemed appropriate.

* * * * * * * * *

We would like to extend our appreciation to Treasury for the cooperation and courtesies extended to our staff during the review. If you have any questions, please call me at (202) 927-6512.

Donald R. Kassel
National Director, *Banking and Fiscal Service*

Our objective was to determine Treasury's responsibilities as the lead Federal agency for the Banking and Finance sector under PDD 63 and to assess the actions Treasury has taken to comply with these responsibilities.

Our limited review included interviews with various Treasury officials, and a review of PDD 63 and related Executive Orders. We obtained information from governmental internet websites, including those of the White House, the FBIIC, the NIPC, FEMA, the Department of Homeland Security, and the Federal banking regulators. We reviewed numerous reports that GAO had issued regarding critical infrastructure protection, especially as it relates to the financial services sector (see Footnote 25), and interviewed GAO staff responsible for some of this work.

We reviewed key publications related to PDD 63, including the PCCIP report to the President titled *Critical Foundations: Protecting America's Infrastructures*, issued during October 1997. We considered the May 2002, Banking and Finance Sector input to the Partnership for Critical Infrastructure Security for *The National Strategy to Secure Cyberspace - Draft for Comment* report. We evaluated the September 2002, PCIPB draft of *The National Strategy to Secure Cyberspace*, and the final strategy, which was released during February 2003 as *The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets.* We also considered Treasury's response to current issues, including its issuance of a circular titled *Treasury Statement on Measures to Protect the Financial Markets During Hostilities with Iraq*.

Our work was conducted at the Department of the Treasury in Washington, D.C., in accordance with the President's Council on Integrity and Efficiency *Quality Standards for Inspection*.

Washington Headquarters

Donald R. Kassel, National Director, *Banking and Fiscal Service*
Maria V. Carmona, Audit Manager
Leslye Burgess, Auditor

Department of the Treasury

Deputy Assistant Secretary, Critical Infrastructure Protection and Compliance Policy
Office of the General Counsel
Office of Strategic Planning and Evaluations
Office of Accounting and Internal Control

Office of Management and Budget

OIG Budget Examiner

Page Intentionally Left Blank