

STATEMENT

OF

RHONDA MACLEAN
PRIVATE SECTOR COORDINATOR
FINANCIAL SERVICES CRITICAL INFRASTRUCTURE PROTECTION
AND HOMELAND SECURITY
&
DIRECTOR, CORPORATE INFORMATION SECURITY
BANK OF AMERICA

BEFORE THE
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS AND THE CENSUS
UNITED STATES CONGRESS

April 8, 2003

TESTIMONY OF RHONDA MACLEAN

Chairman Putman, Ranking Member Clay, and members of the Subcommittee, thank you for inviting me here today to testify at this hearing on “Cyber Security: The Challenges Facing Our Nation in Critical Infrastructure Protection.” I am honored to appear today to speak on behalf of the financial services sector in my role as the Department of Treasury-appointed private-sector coordinator for critical infrastructure protection.

My name is Rhonda MacLean. I am a Senior Vice President at Bank of America Corporation responsible for Corporate Information Security. My responsibilities also include the Bank of America enterprise business continuity planning and the company’s regional recovery centers. This encompasses organizing disaster recovery exercise activities and program capability implementation to ensure the ongoing delivery of services to our customers.

Before joining Bank of America in 1996, I worked for The Boeing Company for 14 years, and as the senior manager for computer and communications security, I was responsible for all commercial airplane and government information security initiatives. I have served in a number of external advisory roles and in professional activities related to information security; I currently serve on the University of North Carolina – Charlotte, Board of Advisors for the College of Information Technology.

Let me first compliment the subcommittee for holding these hearings. Our sector looks forward to working with you as you explore cyber security issues. Today, I plan to provide you with background on the financial services industry’s involvement in critical infrastructure protection efforts, the current work of our Financial Services Sector Coordinating Council, and to discuss opportunities where industry and government can partner to address some of the challenges we face in securing cyber space.

At all levels across our sector, including executive leadership, operations personnel, our trade associations, professional institutes, and our customers, we are very aware of the new global realities and the importance of the vital financial services we provide globally to the nation and our customers.

The Department of the Treasury recently noted, “We continue to work with the financial and banking communities so that our financial system remains functioning efficiently and effectively. We are confident America’s financial

infrastructure is strong and resilient.”¹ There should be no doubt that the public-private partnership is well engaged to ensure the safety, soundness and resiliency of our industry is not only maintained but also enhanced.

In May of 2002, consistent with public-private sector partnership objectives expressed in Presidential Decision Directive 63, subsequent Executive Orders, and the published National Strategies for Homeland Security and Cyber Space Security, I accepted an appointment to serve as the private sector coordinator from the Department of the Treasury, which is the lead agency for the banking and finance sector. To assist me in these responsibilities, Bank of America is demonstrating its well-recognized industry leadership by providing three additional full-time staff resources to support me in carrying out these responsibilities for our industry.

The “National Strategy to Secure Cyber Space,” published by the Administration in February 2003, identified the nation’s critical infrastructures as consisting of the physical and cyber assets of public and private institutions in several sectors: agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping. These infrastructures have been deemed critical because “... their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States.”²

The information technology, telecommunications and electric power industries provide components and services vital to the operation of all these infrastructures. More than ever before, computer technology is imbedded at many levels consisting of servers, routers, and switches and connected by fiber optic cables, wire lines, and wireless technology. We depend upon these systems and components to make our critical infrastructures work. Thus, maintaining the availability and integrity of those mission-critical assets is essential to our economy and our national security.

Those who own and operate these critical Infrastructures maintain the availability and integrity of these system components through the application of a variety of security disciplines, operational controls, and response and contingency initiatives. Though the basic approach to security must fundamentally address the people, process, and technology aspects of the infrastructure implementations, there is no single solution to the security challenges. Because threats and technology continue to change, cyber security approaches and process employed must continuously evolve – this is what is often characterized

¹ Treasury Statement on Measures to Protect the Financial Markets during Hostilities with Iraq, March 17, 2003.

² Executive Order 13010, Critical Infrastructure Protection, July 15, 1996.

as “good practices.”

These “good practices” involve implementation of an appropriate balance of prevention, detection, protection, response and recovery measures. Creating the appropriate balance of these elements is based on operational risk management considerations that address the critical nature of the systems as well as the exposures to which they can be subjected. The wider use of a common enterprise network to conduct business operations creates an architectural model that organizations must recognize and one that requires an enterprise-level risk management governance process.

To address these common enterprise environments, organizations must adjust their decision-making and risk management accordingly. The creation of this “shared risk environment” necessitates an enterprise-wide process and centralization of risk management decisions whenever those decisions could impact the enterprise’s availability or integrity. For large enterprises consisting of many business elements, this is an organizational challenge for those with distributed and multiple business models. The individual businesses may have different risk tolerances but the enterprise network is an area for “shared risk management.” In my view and experience, centralization of an enterprise’s key security services produces the most consistent degree of strong security and improves the ability to effectively monitor and determine enterprise-wide compliance with security practice and appropriate configurations. Our experience with this model has demonstrated significant cost efficiencies while at the same time providing more consistent security.

Historical Perspective

For the past 6 years, infrastructure protection has been the increasing focus of U.S. government policy and initiatives, and encouragement of an active public-private partnership has been a hallmark of their strategy.

Historically, the financial services sector has been a leader in addressing the challenges associated with operating the vast array of information technology and processing inherent throughout the financial services industry. Vigilance and the dedication of significant resources over time have allowed us to develop a wealth of expertise, experience and talent to address issues of security, risk management and protection against crimes such as fraud.

The shift to electronic – and increasing mobile – commerce, extended the need for security to individual customers and to implementing networks, servers, software and other devices.

To address the many recommendations proposed in the President’s Commission on Critical Infrastructure Protection report, an action plan was developed in May 1998: the Presidential Decision Directive (PDD) 63. The primary banking and

finance sector goal established in PDD-63 was to ensure the orderly functioning of the economy and the delivery of essential services.

The private sector working with its lead agency was to contribute to a sector plan, that included:

- Assessing the vulnerabilities of the sector to cyber or physical attacks,
- Recommending a plan to eliminate significant vulnerabilities,
- Proposing a system for identifying and preventing attempted major attacks, and
- Developing a plan for alerting, containing and rebuffering an attack.

Task areas of initial focus by the sector included:

- Vulnerability education and awareness
- Vulnerability analyses
- Creation of a private sector information sharing and analysis center
- Sector research and development needs

Working groups were established by the banking and finance sector to address these goals. This working group recommended creating the Financial Services Information Sharing and Analysis Center (FS-ISAC), a private-sector partnership among eligible financial services companies designed to anonymously share information regarding security incidents, threats, vulnerabilities and solutions. The financial services sector responded by forming the Financial Services Information Sharing and Analysis Center (FS-ISAC). The FS-ISAC, LLC was created to govern the FS-ISAC for the financial services industry. A board of managers, consisting of interested industry information professionals, was formed. The FS-ISAC was launched on October 1, 1999, by its founding members.

In that same period, industry working groups, consisting of representatives from concerned institutions, were examining awareness and education initiatives and efforts to identify the sector's research and development needs.

Further, to address critical infrastructure interdependency issues or cross-sector critical infrastructure issues, the Partnership for Critical Infrastructure Security (PCIS) was founded in 1999. The PCIS's purpose is to promote and ensure reliable critical infrastructures through cross-sector coordination. PCIS provided a forum for different critical infrastructure sectors to collaborate on cross-sector knowledge sharing and coordination.

In July 2002, in response to a government-issued national cyber security strategy, a working group of our sector's institutions developed an initial national strategy document to address critical infrastructure protection.

These initial efforts on critical infrastructure protection were given more national focus as a result of the terrorist attacks on September 11, 2001. The importance

of ensuring rapid recovery and improved resiliency of business functions and telecommunications were given renewed importance.

Additionally, new global realities and threat environment made it necessary to consider the impact of potential situations that could have broad regional consequences. For the financial services sector, many of these new concerns were discussed in a “Draft Interagency White Paper on Sound Practices to Strengthen the Resilience of the U. S. Financial System.” The agencies had reached conclusions regarding “...the necessity to assure the resilience of critical U.S. financial markets in the face of wide-scale, regional disruptions and identified a number of sound practices to strengthen the resiliency of the overall U.S. financial system and the respective U.S. financial centers.”

Most institutions reviewed and enhanced their business continuity efforts in light of these new realities. Collectively, we have been examining and increasing our sector’s ability to provide for business continuity and business resumption against situations that may have regional impacts. Our industry is examining and implementing solutions to some multi-faceted issues in this area, which include economic implications, changes in recovery strategies, new back-up facilities and enhanced telecommunications contingencies.

The new realities and challenges we are facing have caused institutions to organize “executive teams” working in a multi-disciplined manner on physical security, cyber security, life safety, disaster recovery, business continuity and business resumption issues.

At Bank of America, we have such an executive team. Collectively, the team is working to provide integrated leadership to address the new realities. This can be viewed as a microcosm at the institution level of the leadership opportunities also being undertaken at the financial services sector level.

Let me discuss further the telecommunications area. Our sector has been working closely with the telecommunications industry to understand ways to improve redundancy and diversity of telecommunication services that support critical financial services functions.

In the telecommunications area, we are not only concerned with addressing reliability resulting from random system failures, but also “survivability” of telecommunications services from targeted attacks on such infrastructures. This is of increased concern when considering the new global realities. This area provides a prime example of opportunities, including research and development that would help achieve resiliency goals, for both the telecommunications and financial services sectors to partner for their collective benefit.

Let me discuss how our sector level critical infrastructure protection efforts have evolved.

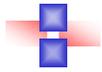
Financial Services Sector Coordinating Council

At the time of my appointment, no single entity could legitimately say it represented the financial services sector. Individual associations were actively and effectively working on their members' behalf to provide tools and resources necessary to enhance infrastructure protection. The associations and their members have provided much leadership for our sector and have done outstanding work on various areas, including crisis management efforts, "good practices" knowledge sharing, business continuity practices, and education and awareness initiatives.

Immediately after my appointment in May 2002, we began forming the Financial Services Sector Coordinating Council, with the public sectors' support and encouragement, and with the leadership of the Department of the Treasury.

The council consists of the primary organizations that, through their constituencies, represent the majority of the financial services sector. These include key national exchanges, clearing organizations, trade associations in the banking, securities, bond, and insurance segments of our industry and key professional institutes.

Today, 24 organizations, listed below, are working together to identify and coordinate strategic initiatives that will improve critical infrastructure protection for our sector and with other sectors upon which we depend. The council is a limited liability corporation that has been institutionalized to carry on the sector's work long after my tenure as sector coordinator is completed. Through our council members, we engage nearly all financial services sector institutions, exchanges and utilities.



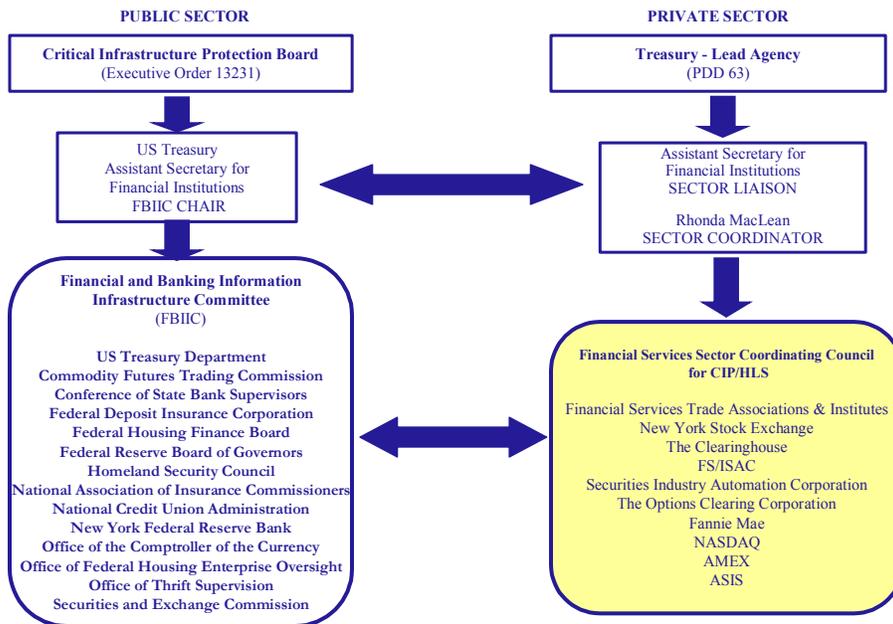
Members

- **ABA** – American Bankers Association
- **ACLI** – American Council of Life Insurers
- **ASIS** – American Society for Industrial Security
- **ACB** – America's Community Bankers
- **BAI** – Bank Administration Institute
- **BITS/FSR** – BITS and The Financial Services Roundtable
- **CUNA** – Credit Union National Association
- **Fannie Mae**
- **CBA** – Consumer Bankers Association
- **FS/ISAC** – Consumer Bankers Association
- **FIA** – Futures Industry Association
- **ICBA** – Independent Community Bankers of America
- **ICI** – Investment Company Institute
- **MFA** – Managed Funds Association
- **NASD** – NASD, Inc.
- **NASQ** – NASDAQ Stock Market, Inc
- **NAFCU** – National Association of Federal Credit Unions
- **NACHA** – National Automated Clearinghouse Association
- **SIA** – Securities Industry Association
- **The BMA** – The Bond Market Association
- **The Clearing House**
- **The OCC** – The Options Clearing Corporation

At the sector level, this is an example of ‘macro’ collective leadership being taken to address the new realities. Through this collective leadership and collaboration, we are leveraging the work being performed across the sector for the benefit of the “common good” of our industry. The council model and approach being taken by our sector is being examined by other national critical infrastructure sectors.

This council provides an efficient approach for coordinating the many and diverse participants that comprise our industry sector. Additionally, because there is a corresponding group within the public sector the Financial and Banking Information Infrastructure Committee (FBIIC), chaired by the Treasury Department, we have the opportunity for direct dialogue on common issues and challenges. The result is an emerging agreement on strategic initiatives we believe will improve infrastructure protection and homeland security.

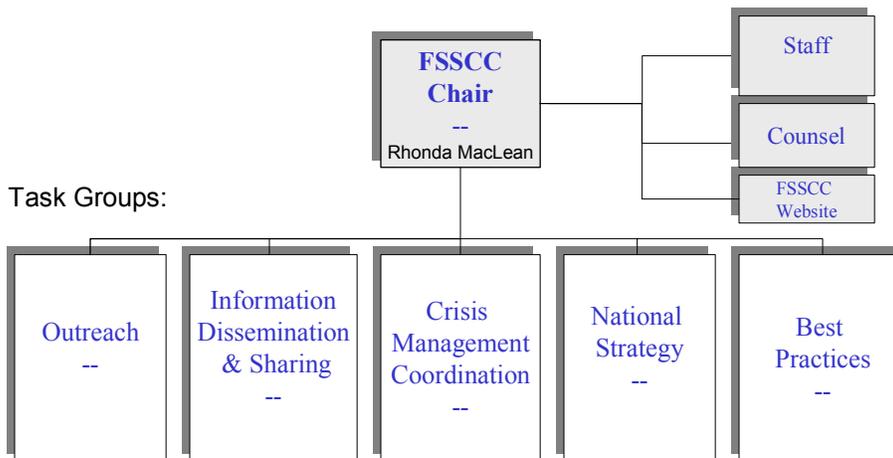
Financial Services Cyber and Physical Protection Framework



© FSSCC, LLC 2003

Five initial strategic areas are the current focus of the council's work. Our approach is to leverage the work already accomplished by our council member organizations to achieve our objectives. Council members are taking primary leadership roles, based on their natural areas of expertise.

Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security



©FSSCC 2003

Information Dissemination and Information Sharing – Our goal is to ensure that a universal service to disseminate trusted and timely information will be available to all sector participants to increase knowledge about physical and cyber security operational risks faced by the financial services sector. Enhancing the needed services provided by our sector’s ISAC is a major focus of our current sector efforts.

Crisis and Response Management – When events occur with broad sector or national impact, a planned and adopted approach for sector-wide crisis management coordination exists, including coordination with government entities. The focus of our efforts is on the ability to communicate and respond as a sector when such events occur.

Sector and Cross Sector Outreach – It is important for each organization to determine how to optimally support and commit efforts for achieving the goals of the executive orders and national strategies. We are developing a strategy for sector-wide outreach on homeland security and critical infrastructure protection initiatives that includes regional forums we are conducting jointly with the FBIIC.

Knowledge Sharing - Best Practices – There are numerous “lessons learned” activities and knowledge sharing of “good practices” within various trade associations and among institutions and government entities. We are developing an organized repository to provide this information to authorized institutions and individuals.

National Strategy – We are also leading the sector’s effort to revise our sector’s “national strategy” document in response to the two national strategies released in February by the President. The strategies are focused on “The Physical Protection of Critical Infrastructures and Key Assets” and “Securing Cyberspace.” This is our opportunity to define strategic as well as tactical, actionable and measurable programming, to direct and advance our sector-wide critical infrastructure and homeland security efforts and to address the recommendations outlined in the national documents strategies referenced above.

In my chairperson role for the FSSCC, I work closely with our lead agency, the Department of Treasury, and the Financial and Banking Information Infrastructure Committee (FBIIC).

It is through council members’ cooperative efforts, their member institutions, and the strong leadership provided by the Treasury and through FBIIC, that we are able to maximize our resources and achieve our objectives to ensure protection of our critical infrastructures to the benefit of the economy and to all financial services customers.

Opportunities

Let me transition and discuss several areas of importance to continuing the progress that has been made by both the government and the private sector.

Information Analysis and Infrastructure Protection

The early critical infrastructure protection visionaries of the 90's clearly understood that raising awareness of these issues was an essential first step. That aspect has been fairly well accomplished. Additionally, addressing holistically both the physical and cyber security aspects of critical infrastructure protection and other issues in response to more sophisticated attacks have now been institutionalized in the Department of Homeland Security (DHS). The need for synergy between information analysis and infrastructure protection has clearly been recognized in the assignment of those responsibilities to an undersecretary within DHS. We expect this to provide a much more robust alerting, threat warning and information flow from the public sector based on the vast resources they have available to integrate.

National Strategy

The National Strategy to Secure Cyberspace correctly recognizes a national effort is required. According to the strategy, "The federal government alone cannot sufficiently defend America's cyberspace. Our traditions of federalism and limited government require that organizations outside the federal government take the lead in many of these efforts. Every American who can contribute to securing part of cyberspace is encouraged to do so. The federal government invites the creation of, and participation in, public-private partnerships to raise cyber security awareness, train personnel, stimulate market forces, improve technology, identify and remediate vulnerabilities, exchange information, and plan recovery operations."³

Understanding the Threat

Based on the governments' visibility of threats to the private sector, a clear understanding of the protection needs must exist between the public and private sector. Gaps between the private sector's protection efforts and the government's view of the necessary protections must be defined and understood. There may be situations where, unknown to the private sector, normal business practices do not adequately address the level of threat understood by the government. Where market forces do not provide the appropriate incentives to provide these protections, augmentation of market mechanisms with such incentives may be appropriate.

Product Security

Because the private sector mainly employs commercial services, products and software to implement cyber security protection and monitoring, those efforts that improve the security of such products have broad benefit. As a sector, we work

³ National Strategy to Secure Cyberspace, February 2003

closely with our vendors to achieve higher levels of security. This is an area that has benefited from both private and public sector efforts. The BITS product certification program is a prime example of our industry's efforts to work closely with the product vendors to meet common criteria and minimum acceptable security standards established by the financial services industry.

Skilled Workforce

In all areas of cyber security, having the best-trained and skilled people is essential to engendering a leadership position for a company and the nation.

The Computing Technology Industry Association commissioned a recent study, the results of which strongly suggest that more training and certification for IT professionals will help America become better protected against mounting cyber threats.

Any incentives and encouragement that bolsters the available talent pool of software developers with a strong security component of their training should result in improved software products.

Voluntary Sharing of Threat and Incident Information

And finally, we must continue to encourage processes that accommodate companies' voluntary sharing of sensitive information, such as the provisions outlined in the Homeland Security Act of 2002. Such provisions of the Critical Information Infrastructure Act of 2002 encourage sharing by providing companies with necessary Freedom of Information Act (FOIA) protections, without giving up the option for government to pursue legal and regulatory action when necessary.

Summary

In summary, our industry is focused on protecting the integrity of the infrastructure for physical as well as electronic delivery of financial services. We have taken steps to ensure the global architecture for financial transactions is as safe, secure and sound as possible.

Our sector has evolved its sector-wide efforts and has committed to a formal structure and entity, the Financial Services Sector Coordinating Council, to foster and facilitate the coordination of financial services sector-wide voluntary activities and initiatives designed to improve Critical Infrastructure Protection and Homeland Security.

We are committed to a close public-private partnership to address the new global realities we face as a nation. Where market forces do not adequately address the threats the public sector has identified, appropriate incentives must be structured for those services critical to the national security and national and global economic prosperity. Also, continuing to provide the legal and legislative

mechanisms that permit the exchange of sensitive infrastructure protection information with the government is an essential element of the partnership.

Continually improving commercial product security and increasing the required pool of talented and trained personnel to meet the security development and implementation demands of the innovative information technology all infrastructures employ is a challenge for us all.

Mr. Chairman and Members of the Committee, we believe the strong public/private sector partnership that is emerging is the right approach. The FSSCC would be happy to work with your Committee, staff and other Members of Congress to discuss aspects of the testimony in greater detail.

Thank you for this opportunity to testify.

About the Financial Services Sector Coordinating Council for Critical Information Protection and Homeland (CIP/HLS)

The Financial Services Sector Coordinating Council for CIP/HLS fosters and facilitates financial services sector-wide activities and initiatives designed to improve Critical Infrastructure Protection and Homeland Security. The council was created in June 2002, by the private sector, with recognition from the U.S. Treasury, to coordinate critical infrastructure and homeland security initiatives for the financial services industry. The five major areas of immediate focus for the council include: Effective and Rapid Information Dissemination; Crisis Management and Response Coordination; Outreach and Organizational Engagement; Knowledge Sharing and Best Practices and the National Strategies for Homeland and Cyber Security.

About Bank of America

One of the world's leading financial services companies, Bank of America is committed to making banking work for customers and clients like it never has before. Through innovative technologies and the ingenuity of its people, Bank of America provides individuals, small businesses and commercial, corporate and institutional clients across the United States and around the world new and better ways to manage their financial lives. The company enables customers to do their banking and investing whenever, wherever and however they choose through the nation's largest financial services network, including approximately 4,400 domestic offices and 13,000 ATMs, as well as 30 international offices serving clients in more than 150 countries, and an Internet Web site that provides online banking access to 4 million active users, more than any other bank.