



Critical Infrastructure Protection in the National Capital Region

**Risk-Based Foundations for Resilience and
Sustainability**

**Final Report, Volume 8:
Banking and Finance Sector**

September 2005

University Consortium for Infrastructure Protection

Managed by the
Critical Infrastructure Protection Program
School of Law
George Mason University

This Page Intentionally Blank

Critical Infrastructure Protection in the National Capital Region

Risk-Based Foundations for Resilience and Sustainability

Final Report, Volume 8: Banking and Finance Sector

Submitted in fulfillment of:

Department of Homeland Security Urban Areas Security Initiative (UASI) Grant 03-TU-03; and
Department Justice Office of Community Oriented Policing Services (COPS) Grant 2003CKWX0199

September 2005

Gerald Hanweck, Lee Zeichner, and Benjamin Stafford

University Consortium for Infrastructure Protection

Managed by the
Critical Infrastructure Protection Program
School of Law
George Mason University



– **Notice** –

This research was conducted as part of the National Capital Region Critical Infrastructure Project, carried out by the University Consortium for Infrastructure Protection, managed by the Critical Infrastructure Protection Program, George Mason University, John A. McCarthy, Director and Principal Investigator.

It was sponsored by the U.S. Department of Homeland Security's Urban Area Security Initiative grant #03-TU-03, and by the U.S. Department of Justice Community Oriented Policing Services Program grant #2003CKWX0199, under the direction of the Senior Policy Group of the National Capital Region.

The views expressed are those of the authors, and do not necessarily reflect the views of the Department of Homeland Security, the Department of Justice, or the Senior Policy Group of the National Capital Region.

Copyright © 2005 by George Mason University

Published in 2006 by George Mason University

Table of Contents

Executive Summary	1
1. Sector Background	4
1.1 Sector Profile	6
1.1.1 General	6
1.1.2 Definitions.....	6
1.1.3 Features	8
1.2 Regional Sector Characteristics	9
1.2.1 Service Areas	9
1.3 Review of Authorities	10
1.4 Mapping of Interdependencies.....	14
1.4.1 Upstream Sectors	15
1.4.2 Downstream Sectors	16
1.4.3 Sidestream Sectors	17
1.4.4 Other Dependencies.....	17
2. State of Security Assessment	17
2.1 Awareness of value of CIP and CIVA/RM.....	17
2.2 Availability of appropriate tools (open source or proprietary)	18
2.2.1 Vulnerability assessments	18
2.2.2 Compliance-oriented policies and procedures	18
2.2.3 Risk management methods	22
2.3 Allocation of resources to CIVA/RM	22
2.4 Extent of implementation of CIP measures	22
2.5 Extent of evaluation of CIP effectiveness.....	23
3. Risk Reduction Programs and Processes	23
3.1 Risk Reduction Project and Investment Recommendations	23
3.1.1 Tactical steps for immediate benefit on the ground.....	23
3.1.2 Strategic steps for long-term benefit on the ground	24
3.2 Risk reduction process improvements	24
3.2.1 Recommendations for enhancements in general guidelines and best practice compliance standards	24
3.2.2 Recommendations for enhancements in risk management	24
3.3 Specific recommendations for governance at the sector-level	24
3.3.1 Incentives	24
3.3.2 Organization and management.....	25
3.4 Specific recommendations addressing dependencies	25
3.4.1 Intra-sectoral	25
3.4.2 Inter-sectoral.....	26
3.4.3 Regional	26
3.5 Measuring Effectiveness.....	26
3.6 Managing Continuous Improvement	26
4. Conclusion	26
4.1 Overarching Findings.....	26
4.2 Challenges.....	27

Appendix A: Methodology for Data Gathering and Analysis	29
Appendix B: Focus Group Participants	30
Appendix C: Review of Open Source VA/RM Tools, Procedures and Processes	31
Appendix D: Upstream and Downstream Sectors	40
Appendix E: 911 Recommendations Implementation Act: Private Sector Preparedness.....	46
Appendix F: Bibliography	49
Appendix G: Definitions.....	52
Appendix H: Acronyms	53
Appendix I: Endnotes	54

List of Figures

Figure1: Banking and Finance Facilities	6
---	---

List of Tables

Table 1: Deposits and Number of All FDIC Insured Institutions Washington, D.C, Metropolitan Statistical Area	9
Table 2: Upstream Sectors.....	15
Table 3: Downstream Sectors.....	16
Table 4: Sidestream Sectors.....	17

Banking and Finance Sector Report

Executive Summary

The state and direction of the critical infrastructure, with regard to the banking and finance sector of the National Capital Region (NCR), is the focus of this report. The approach to providing protection for this sector within the NCR is through a private/public regional partnership.

As this study has developed, it became clear that firms can and have a competitive incentive to become internally efficient in protecting their individual infrastructure. However, as was evident during 9/11, and the hurricanes of 2003 and 2004 that swept from Florida to the Northeast, along with the blackout that hit New York and the Northeast in 2003, there is a need for cooperation with the telecommunications and energy providers, and with government so that business continuity plans, so carefully devised, could be put into operation. To best achieve individual business continuity plans, financial service firms and their government regulators, recognize that a regional organization of these firms, and government agencies, is an efficient way to proceed. Because most crises from terrorist attacks or natural calamities are regional, regional cooperation is best achieved by securing public confidence in the financial services sector. Loss of public confidence in the banking and finance sector, institutions and markets, may cause panic and might potentially impose large economic losses.

An integral part of this sector is the federal and state regulatory and supervisory community; Communities rely on its economy via the payments system; and any severe adverse economic consequence would result in loss of public confidence in the financial system. Federal regulatory agencies, such as the Federal Reserve Board, Office of Comptroller of the Currency, Federal Deposit Insurance Corporation, Office of Thrift Supervision, National Credit Union Administration, Securities and Exchange Commission, Commodities Futures Trading Commission and the Treasury Department, are all located in the National Capital Region. Moreover, they are concentrated within a small radius that includes the White House. This geographical concentration is alleviated to some degree by the geographic dispersion of regional offices of the federal banking regulators, located in major metropolitan areas, but also dispersed throughout state regulatory bodies.

As a mitigation measure, financial institutions have built redundancy and backup processes into their systems and operations. For example, the fact that backup data centers are located in remote areas of the country, usually far from the headquarters or main operations center of a firm, makes the maintenance of secure telecommunications links in time of crisis imperative.

Evidence from focus group meetings of sector regulators and firms, suggests that individual companies and regulatory agencies are well prepared to maintain an adequate degree of business continuity in the event of a crisis. What is lacking in many regions, the NCR included, is coordination and cooperation among firms and the local and federal government units charged with conducting and leading critical infrastructure protection and crisis management and recovery. For example, in the NCR, these focus groups of financial service firms and federal and state regulators agreed that a credentialing process for incidents and planned events, which would be of immediate benefit to the banking and finance sector, does not exist; further, a credentialing has not been planned, nor is there anyone to facilitate this coordination.

Overarching Findings

- Based on an extensive literature review, there is no single repository of vulnerability assessments (VA's) for the banking and finance sector. The federal regulatory agencies have consistently been responsible for oversight of financial service companies and are under mandate to keep the system informed, examined and enforced with regard to issues of critical infrastructure protection.
- In general, VA requirements depend on the kind of financial institution and regulator requirements, e.g., credit union examiners questions for business continuity or information security will be considerably different than examiners of large, global banking companies.
- In as much as the vulnerability assessment tools are those used uniformly by the banking and finance industry and reviewed by the regulators in a coordinated process, the strengths and weaknesses are uniform among companies. The greatest strength and weakness in these tools are that they are firm-specific and system-wide only in the rules and regulations of the payments system.
- There are a significant number of tools, questionnaires, and audit materials available. In some cases, the Federal Financial Institutions Examination Council (FFIEC) provides useful, integrated VA management program, with assessment questions; in other cases, private sector and/or public-private partnerships have produced frameworks for the especially complex issues (e.g., outsourcing and telecom diversity).
- From the literature review and focus groups, there is no shortage of security and vulnerability assessment-related questions and protocols for the banking and finance sector in the NCR that may be relied on for critical infrastructure vulnerability assessment/risk management (CIVA/RM).
- Credentialing is a major problem within the financial services sector of the NCR (identified by focus groups). Importantly, banking and finance personnel must be able to access restricted areas in order to maintain or restore operations during and immediately after an emergency.
- A regional coalition in the NCR is necessary to build cooperation relevant to homeland security and critical infrastructure protection among banking and finance firms. This coalition should include banking and finance regulators; those critical to business continuity; and those in appropriate federal, state, and local government agencies. A good model, ChicagoFIRST, is relevant largely because of its development and implementation of a single point of contact, and its establishment of a communication structure among institutions, governmental bodies, and first responders. ChicagoFIRST has been, and continues to be, a successful model for homeland security and critical infrastructure protection.
- A regional approach, such as the ChicagoFIRST model, is necessary to build cooperation among the banking and finance sector firms, their regulators, and those critical to its business continuity and appropriate federal, state and local government agencies in the NCR.
- Banking and finance companies do not have relationships with federal, state and local government bodies who are in charge of responding to an emergency, such as FEMA, local police, military, state and local transportation departments. This is also true with regard to interrelationships of the banking and finance sector with telecommunications and energy companies. It is in this area that regulatory agencies cannot improve CIP effectiveness, but can only make recommendations.

- There is a need for private sector tabletop exercises that focus on interdependencies among critical infrastructures and state and local jurisdictions in the NCR. These should be done at the physical, cyber, state and regional levels.

Recommendations

- Collaborate with the Department of Homeland Security's (DHS) Office of the National Capital Region Coordination to extend federal credentialing to the banking and finance sector
- Improve coordination, cooperation, and communication within the financial services sector by adopting ChicagoFIRST as a model for the NCR.
- Improve reliability and resiliency of dependencies with other sectors, such as telecommunications and energy in the NCR.
- Coordinate, through the DHS, and fund interdependency tabletop exercises at the physical, cyber, state and regional levels, emphasizing the private sector, critical infrastructures and interdependencies in the NCR.

1. Sector Background

The NCR banking and finance sector, like the rest of the industry, is critical to global, national and regional economies. Nationwide, the sector consists of thousands of banking, thrift, credit union, insurance, stock and real estate brokerage, investment banking offices, stock and futures, options exchanges, and federal and state financial regulatory and supervisory structure. An integral part of this sector is the federal and state regulatory and supervisory community, because of the reliance of the economy on the payments system and the severe adverse economic consequences of the loss of public confidence in the financial system. The federal regulatory agencies, such as the Federal Reserve Board, Office of Comptroller of the Currency, Federal Deposit Insurance Corporation, Office of Thrift Supervision, National Credit Union Administration, Securities and Exchange Commission, Commodities Futures Trading Commission and the Treasury Department, are all located in the National Capital Region, close to the White House. This high degree of geographical concentration is only partially alleviated by the geographic dispersion of the regional offices of the federal banking regulators, with regional offices located in major metropolitan areas and its wide dispersion of state regulatory bodies.

Consequently, the infrastructure of the financial services sector consists of a variety of physical structures, such as buildings and financial utilities, cyber and human capital. Much of the sector's activities and operations take place in large commercial office buildings in large financial and commercial centers, while others are in smaller buildings and locations geographically dispersed. The physical structures to be protected contain retail or wholesale banking operations, financial markets, regulatory institutions, and physical repositories for documents and financial assets. Today's financial services companies conduct the payments and clearing and settlement systems and are primarily electronic, although some physical transfer of assets, such as checks and cash, still occur. This infrastructure includes such electronic systems as computers, digital storage devices, and telecommunication networks. In addition to the sector's key physical components, many financial services employees have highly specialized skills and are, therefore, considered essential elements of the industry's critical infrastructure.

When public confidence in the financial system becomes eroded, as with 1929 stock market crash; economic decline ensues. This realization forms the fundamental reason for financial regulation of depository institutions, the payments system, and securities firms and markets. Thus, the effectiveness of the financial services industry depends on continued maintenance of public confidence and involvement to maintain normal operations. In times of crisis or disaster, maintaining public confidence demands that financial institutions, financial markets, and payment systems remain operational or that their operations can be quickly restored. This need for the maintenance of business continuity guides regulatory requirements for financial firm preparedness and cyber security and management strategies for dealing with crises.

Federal and state regulatory communities and the Department of the Treasury have developed emergency communications plans for the banking and finance sector. With regard to retail financial services, physical assets are well distributed geographically throughout the nation. The sector's retail niche is characterized by a high degree of substitutability, which means that one type of payment mechanism or system can be readily replaced with another during a short-term

crisis. For example, in retail markets, consumers can make payments through cash, checks, or credit and debit cards and offices are geographically dispersed.

The banking and finance sector relies on several critical infrastructure industries for continuity of operations, including telecommunications, electric power, transportation, and public safety services. The sector relies especially on computer networks and telecommunications systems to assure the availability of its services. The potential for disruption of these systems is an important concern. For example, the equity securities markets remained closed for four business days following 9/11, not because any markets or market systems were inoperable, but because the telecommunications lines in lower Manhattan that connect key market participants were heavily damaged and could not be restored immediately. As a mitigation measure, financial institutions have made great strides to build redundancy and backup into their systems and operations. The fact that backup data centers are located in remote areas of the country, usually far from the headquarter office or main operations center, makes the maintenance of secure telecommunications links in time of crisis imperative.

Evidence from focus groups of the banking and finance sector regulators and firms, suggests that individual companies and regulatory agencies are well prepared internally to maintain a workable degree of business continuity in the event of a crisis. Lacking in many regions (the NCR included), however, is coordination and cooperation among firms and the local and federal government units charged with conducting and leading critical infrastructure protection and crisis management and recovery. For example, in the NCR, our focus groups considering financial service firms and federal and state regulators, all agreed that a credentialing system must be put in place to ensure that key employees and management can reach business locations and be informed of safe transit, but none exists and none is planned.

In this regard, the endorsement of the 9/11 Commission of the American National Standards Institute (ANSI) National Preparedness Standard establishes a common set of criteria and terminology for preparedness, disaster management, emergency management, and business continuity programs. One of these recommendations is to leverage public/private partnerships. The principal recommendation for substantial improvement in securing the critical infrastructure of the NCR banking and finance sector is to develop a regional partnership of financial services firms, including non-financial firms representing sectors critical to the financial services sector, such as telecommunications and energy; and federal, state and local government agencies responsible for the regulation of the banking and finance sector; and crisis management and recovery all need consideration.

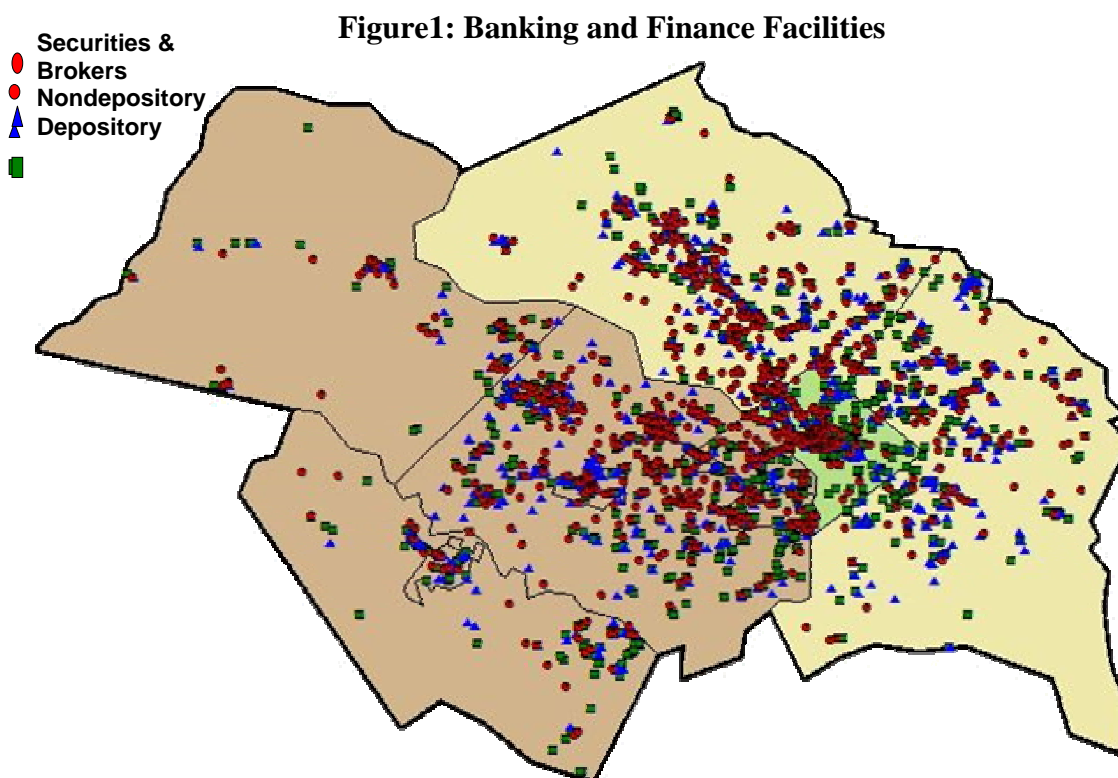
The remainder of this report provides background information about the banking and finance sector and its critical infrastructure nationally and in the NCR. In the final section, several recommendations are proposed to substantially improve the security of the sectors' critical infrastructure and its recovery after a crisis. From the evidence accumulated in this study, particularly from the extensive literature review and focus groups of industry experts and regulators, a private/public sector regional approach is necessary to build cooperation among the banking and finance sector firms and their regulators with those sectors critical to its business continuity and appropriate federal, state and local government agencies.

1.1 Sector Profile

1.1.1 General

The National Capital Region

Officially, the National Capital Region consists of 12 jurisdictions: “The geographic area located within the boundaries of (A) the District of Columbia, (B) Montgomery and Prince George’s Counties in the state of Maryland, (C) Arlington, Fairfax, Loudoun, and Prince William Counties and the City of Alexandria in the Commonwealth of Virginia, and (D) all cities and other units of government within the NCR geographic areas.”¹



1.1.2 Definitions

Banking and Finance: A critical infrastructure characterized by entities, such as retail and commercial banking organizations, investment banking institutions, stock and futures exchanges, securities and commodities brokers, trading companies, insurance and reinsurance companies, reserve systems, associated operational organizations, government operations, and support activities, that are involved in all manner of monetary transactions, including its storage for safe keeping purposes, its investment for income purposes, its exchange for payment purposes, and its disbursement in the form of loans and other financial instruments.²

For the financial and banking sector infrastructures, key risk factors include:

1. **Wide-Scale Disruption**— An event that causes a severe disruption or destruction of transportation, telecommunications, power, or other critical infrastructure components across a metropolitan or geographic area and the adjacent communities that are economically integrated with it; or that results in a wide-scale evacuation or inaccessibility of the population within normal commuting range of the disruption’s range.
2. **Systemic Risk**—The risk of system-wide failure or serious disruption, and includes the risk that the failure of one participant in a transfer system or financial market to meet its required obligations, will cause other participants to be unable to meet their obligations when due, causing significant liquidity or credit problems, or threatens the stability of financial markets and the payments system. Given the complex interdependencies of financial markets, including its participants, thorough preparations by key market participants will reduce the potential that a sudden disruption experienced by one or few firms will cascade into market-wide or regional liquidity dislocations, solvency problems, and severe operational inefficiencies, threatening economic stability, and public confidence.

Core institutions affected by those risks of disruption or failure are:

1. **Financial Markets**—Well functioning and unimpaired financial markets provide the means for banks, securities firms, the Federal Reserve System, Treasury and other financial institutions, to adjust their cash and securities positions, and those of their customers and general market, in order to manage liquidity, market and other risks to their organizations, and to provide credit to customers. Financial markets also provide support for a wide range of financial services to businesses and consumers in transactions, which by the end of the business day, could present systemic risk. While there are different ways to gauge the degree of criticality of such firms in financial markets, as a guideline, the financial regulatory agencies consider a firm significant in a particular market if it consistently clears or settles at least 5% of the value of transactions in the market. However, absolute size, location and visibility are also as important because companies, such as Citigroup or JP Morgan, if seen as weakening due to financial market disruption, then public confidence might be shaken even though they may not be headquartered in such regions as the NCR.
2. **Core Clearing and Settlement Organizations**—Core clearing and settlement organizations consist of two groups of organizations that provide clearing and settlement services for critical financial markets or act as large-value payment system operators and present systemic risk should they be unable to perform. The first group consists of market utilities (government-sponsored services or industry-owned organizations) whose primary purpose is to clear and settle transactions for critical markets or transfer large-value wholesale payments. The second group consists of those private-sector firms that provide clearing and settlement services that are integral to a critical market (i.e., their aggregate market share is significant enough to present systemic risk in the event of sudden failure to carry on those activities because there are no viable immediate substitutes).

For this research, the terms “recovery” and “recover” refer to the restoration of clearing, settlement and cash provision activities after a wide-scale disruption; resumption (or resume)

refers to the capacity to accept and process new transactions and payments after a wide-scale disruption.

Recovery and Resumption of Clearing and Settlement and Financial Sector Activities—the rapid recovery and resumption of critical financial markets, and the avoidance of potential systemic risk and loss of public confidence in the financial sector, requires the rapid recovery of clearing and settlement activities. These are necessary to meet customer financial transaction requirements and to complete pending transactions on scheduled settlement dates. Clearing and settlement activities include:

- a. Completing pending large-value payments
- b. Clearing and settling all other pending transactions
- c. Meeting end-of-day funding and collateral obligations necessary to ensure the performance of items (a) and (b) above
- d. Managing open firm and customer risk positions, as appropriate and necessary, to ensure the performance of items (a) through (c) above
- e. Communicating firm and customer positions, providing services to customers, particularly cash, debit and credit card transactions, debit and credit balances, and reconciling the day's records, and safeguarding firm and customer assets as necessary to ensure the performance of items (a) through (d) above
- f. Carrying out all support and related functions that are integral to performing the above critical activities, such as the Federal Reserve System.

1.1.3 Features

According to flow-of-funds statistics from the Federal Reserve Board,³ U.S. financial institutions held more than \$28 trillion in assets as of fourth quarter 2004—about a \$2 trillion dollar increase over the fourth quarter 2003. The largest financial institutions are commercial banks (\$6.5 trillion), insurance companies (\$3.4 trillion), mutual funds (\$3.9 trillion), government-sponsored enterprises (\$2.6 trillion), and public and private pension funds (\$1.5 trillion). The remaining assets are distributed among savings institutions (S&L's), credit unions, finance and mortgage companies, securities brokers and dealers, and other financial institutions. In total, financial institutions, including those that make up the banking and financial sector, hold 76.2% of the total financial assets in the U.S. economy.

Composition of the financial services sector extends beyond holding and investing in financial assets, to include a network of essential, specialized financial service organizations and service providers, who support the sector in its efforts to provide a trusted services environment. These include:

- Securities and commodities, and futures exchanges
- Funds transfer networks
- Payment networks
- Clearing companies, trust and custody firms
- Depositories and messaging systems.

Literally trillions of dollars of transactions will flow through these institutions daily, including the flow of funds arising from the payments system. Furthermore, like many companies and government bodies, the financial services sector has also become more dependent on outsourcing certain activities—such as systems and applications, hardware and software, as well as

technically-skilled personnel—to third-party providers that are an indispensable part of the sector’s infrastructure.

The financial services sector is highly regulated, from both a state and federal level. Several regulatory agencies oversee various aspects of the financial services industry. For instance, banks, thrifts and credit unions are regulated by five federal regulators—the Federal Reserve System (FED), the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC), the Office of Thrift Supervision (OTS), and the National Credit Union Administration (NCUA).

For banks and thrifts, the FED, FDIC, OCC and OTS, supervise and examine all federally-insured depository institutions, regardless of federal or state charter (OCC, OTS and NCUA regulate federally-chartered banks, thrifts and credit unions, respectively). Regulators oversee a mix of global large, medium, and small depository institutions. Banking regulators work together through the Federal Financial Institutions Examinations Council (FFIEC),⁴ an interagency forum Congress established in 1979, to promote consistency in the examination and supervision of depository institutions. For example, the members of the Information Technology Subcommittee of the FFIEC Task Force on Supervision, supervise the largest 18 to 20 technology service providers, and, through the regulators’ regional offices, supervise smaller technology service providers.

These regulators also issue policies, procedures, rules, legal interpretations, and corporate decisions concerning banking, credit, bank investments, asset management, fair lending and consumer protection, community reinvestment activities, and other aspects of bank operations.

1.2 Regional Sector Characteristics

1.2.1 Service Areas

The NCR is the sixth largest banking market in the U.S. by total deposits, just behind Philadelphia and San Francisco. In total, the NCR has 99 independent banks and thrifts with 1,455 separate offices (not including ATM’s) (see Table 1 below). The three largest headquarters locations, controlling 35% of deposits are Charlotte, N.C. (Wachovia), Charlotte, N.C. (Bank of America), and Miami, F.L. (SunTrust). The depository institutions nationally have nearly \$900 billion in deposits compared to the \$120 billion in the NCR. Of the 99 banking organizations in the NCR, 15 are headquartered outside of D.C., Maryland, and Virginia.

Table 1: Deposits and Number of All FDIC Insured Institutions Washington, D.C, Metropolitan Statistical Area

MSA as of June 30, 2004	All Institutions			Commercial Banks			Savings Institutions		
	Number of		Deposits	Number of		Deposits	Number of		Deposits
	Institutions	Offices		Institutions	Offices		Institutions	Offices	
Washington DC MSA	99	1,455	119,795	80	1,198	76,390	19	257	43,405

(Dollar values in millions)

Source: FDIC, Summary of Deposits, June 30, 2004

The number of life, and property and casualty insurance companies offering products and services within the NCR number about 145 at about 2,400 locations, according to

YellowPages.com. In addition, there are 62 Savings and Loan Associations (S&L's) and credit unions offering deposit services in the NCR.

1.3 Review of Authorities

Banking and finance sector firms are highly regulated at the state and federal levels. For instance, there are numerous state and federal laws that govern firms that offer financial services, but most important to the critical infrastructure of this sector are those that give power to the state and federal government to examine these firms through on-site visits for purposes of firm safety and soundness. With this examination power, state and federal governments can, recommend and enforce security and business continuity measures needed at the firm level.

As mentioned, the banking and finance sector industry is highly regulated and competitive. Industry professionals, management and government regulators regularly engage in identifying sector vulnerabilities and take appropriate prescribed protective measures, including sanctions imposed on institutions that do not consistently meet those prescribed standards.

State Regulators and Chartering

The *Bureau of Financial Institutions* is a regulatory division of the Virginia State Corporation Commission. The bureau is headed by a commissioner; and each commissioner oversees a type of financial institution. The Bureau of Financial Institutions is divided into five sections:

1. **Banks and Savings Institutions** - examines and supervises state-chartered banks and thrift institutions.
2. **Consumer Finance** - examines and supervises industrial loan associations, consumer finance companies, mortgage lenders and brokers, credit counseling agencies, money order sellers, money transmitters and check cashers.
3. **Credit Unions** - examines and supervises state-chartered credit unions.
4. **Corporate Structure and Research** - investigates applications filed with the SCC by banks and other financial services companies, and conducts economic research.
5. **Administration and Finance** - provides logistical support to the regulatory sections, administers human resource, financial and automated operations, maintains bureau records, and handles consumer complaints.

The Washington D.C. Department of Insurance, Securities and Banking (DISB) regulates financial service firms operating in the District of Columbia; by law, all FDIC insured banking and thrift companies must be nationally chartered by either the OCC or OTS, which are the primary regulators.

DISB regulates the following entities: insurance companies, insurance producers, health maintenance organizations, captive insurance companies, and risk retention groups; securities businesses, investment advisors, investment representatives, brokers, dealers, agents of issuers operating securities businesses; banks, mortgage lenders and brokers, check cashers, money transmitters, consumer sales finance companies, money lenders, and consumer credit service organizations.

The Maryland Commissioner of Financial Regulation is the primary regulator for many state-chartered financial institutions, including, banks, credit unions, and trust companies; and state-

licensed financial entities such as, consumer finance companies, mortgage lenders and brokers, consumer debt collection agencies, check cashers, and money transmitters.

The commissioner supervises the activities of these businesses to ensure compliance with the financial institution laws and regulations of Maryland. Supervision includes periodic on-site examinations, as well as, off-site monitoring programs.

Federal Regulators

A unique feature of each of the organizations referred to below is that they are headquartered and have their primary policy making operations within the NCR. Because it is imperative that they are each operational during crisis management and recovery in time of regional or national catastrophe, each is integral to the critical infrastructure of the NCR as well as the nation.

The Federal Reserve System (FED)

The FED is the central bank of the United States. It was founded by Congress in 1913 to provide the nation with a safer, more flexible, and more stable monetary and financial system. Over the years, its role in banking and the economy has expanded.

The Federal Reserve's duties are within four general areas:

1. Conducting the nation's monetary policy by influencing the money and credit conditions in the economy in pursuit of full employment and stable prices
2. Supervising and regulating banking institutions to ensure the safety and soundness of the nation's banking and financial system and to protect the credit rights of consumers
3. Maintaining the stability of the financial system and containing systemic risk that may arise in financial markets
4. Providing certain financial services for the U.S. government, the public, financial institutions, and for foreign official institutions, including playing a major role in operating the nation's payments system.

It is in all four of these areas that the FED is integral to any critical infrastructure protection policy that may be adopted nationally or for the NCR.

The Office of the Comptroller of the Currency (OCC)

The OCC charters, regulates, and supervises all national banks. It also supervises the federal branches and agencies of foreign banks. Headquartered in Washington, D.C., the OCC has four district offices, plus an office in London to supervise the international activities of national banks.

The OCC was established in 1863 as a bureau of the U.S. Department of the Treasury. It is headed by the comptroller, who is appointed by the president, with the advice and consent of the Senate, for a five-year term. The comptroller also serves as a director of the Federal Deposit Insurance Corporation (FDIC) and a director of the Neighborhood Reinvestment Corporation.

The OCC's nationwide staff of examiners conducts on-site reviews of national banks and provides sustained supervision of bank operations. The agency issues rules, legal interpretations, and corporate decisions concerning banking, bank investments, bank community development activities, and other aspects of bank operations.

In regulating national banks, the OCC has the power to:

- Examine federally-chartered banks to ensure the safety and soundness of the national banking system and to foster competition by allowing banks to offer new products and services. Security of the institution, records and funds is a primary concern.
- Approve or deny applications for new charters, branches, capital, or other changes in corporate or banking structure.
- Take supervisory actions against banks that do not comply with laws and regulations or that otherwise engage in unsound banking practices. The agency can remove officers and directors, negotiate agreements to change banking practices, and to issue cease and desist orders as well as civil money penalties.
- Issue rules and regulations governing bank investments, lending, and operational practices that may be related to protection of banking infrastructure and the establishment of standards for banks doing so.

The Office of Thrift Supervision (OTS)

OTS is the primary regulator of all federally chartered and many state-chartered thrift institutions, which include savings banks and savings and loan associations. OTS was established as a bureau of the U.S. Department of the Treasury on August 9, 1989, is headquartered in Washington, D.C., and has four regional offices located in Jersey City, Atlanta, Dallas, and San Francisco. OTS is funded by assessments and fees levied on the institutions it regulates.

The Federal Deposit Insurance Corporation (FDIC)

FDIC preserves and promotes public confidence in the U.S. financial system by insuring deposits in banks and thrift institutions for up to \$100,000; by identifying, monitoring and addressing risks to the deposit insurance funds; and by limiting the effect on the economy and the financial system when a bank or thrift institution fails. It is located in Washington, D.C. and conducts much of its examination business in six regional offices and in field offices around the country.

An independent agency of the federal government, the FDIC was created in 1933 in response to the thousands of bank failures in the early 1930's.

The FDIC receives no Congressional appropriations – it is funded by premiums that banks and thrift institutions pay for deposit insurance coverage and from earnings on investments in U.S. Treasury securities. With insurance funds totaling more than \$44 billion, the FDIC insures more than \$3 trillion of deposits in U.S. banks and thrifts – deposits in virtually every bank and thrift in the country.

The FDIC directly examines and supervises about 5,300 state chartered banks and savings banks, which includes more than half of the institutions in the banking system. In addition, the FDIC is the back-up supervisor for the remaining insured banks and thrift institutions.

The National Credit Union Administration (NCUA)

NCUA is the independent federal agency, located in Alexandria, Virginia, that charters and supervises federal credit unions. NCUA, backed by the full faith and credit of the U.S.

government, operates the National Credit Union Share Insurance Fund (NCUSIF), insuring the savings of 80 million account holders in all federal credit unions and many state-chartered credit unions.

The Federal Financial Institutions Examination Council (FFIEC)⁵

Although not a regulatory body, the council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the board of governors of the Federal Reserve System (FED), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS), and to make recommendations to promote uniformity in the supervision of financial institutions.

Of importance to the critical infrastructure protection of the banking and finance sector, FFIEC, in cooperation with all the federal bank regulatory agencies and state regulatory bodies, has developed several “IT Booklets” that provide guidance to examiners and financial institutions on the characteristics of an effective information technology (IT) function. In general, the booklets describe the roles and responsibilities of the banking company boards of directors, management, and internal or external auditors; identifies effective practices for IT programs; and details examination objectives and procedures for security and safety and soundness.

The U.S. Securities and Exchange Commission (SEC)

The SEC is the principal U.S. securities regulator with the primary mission to protect investors and maintain the integrity of the securities markets. As more and more first-time investors turn to the markets to help secure their futures, to pay for homes, and send children to college, these goals are more compelling than ever.

The SEC oversight responsibilities of key participants in the securities industry, includes stock exchanges, broker-dealers, investment advisors, mutual funds, and public utility holding companies. Moreover, the commission is concerned primarily with promoting disclosure of important information, enforcing the securities laws, and protecting investors who interact with these various organizations and individuals.

Though it is the primary overseer and regulator of the U.S. securities markets, the SEC also works closely with many other institutions, including Congress, other federal departments and agencies, the Federal Reserve Board, self-regulatory organizations (e.g., the stock exchanges), state securities regulators, and various private sector organizations.

The Commodity Futures Trading Commission (CFTC)

CFTC protects market users and the public from fraud, manipulation, and abusive practices related to the sale of exchange traded commodity and financial futures and options, and to foster open, competitive, and financially sound futures and option markets. The CFTC monitors markets and market participants closely by maintaining, in addition to its headquarters office in Washington, offices in cities that have futures exchanges—New York, Chicago, Kansas City, and Minneapolis.

Congress created the CFTC in 1974 as an independent agency with the mandate to regulate commodity futures and option markets in the United States. The CFTC encourages the competitiveness and efficiency of these markets by ensuring their integrity, protecting market participants against manipulation, abusive trading practices, and fraud, and ensuring the financial integrity of the clearing process. Through effective oversight, the CFTC enables the futures markets to serve the important function of providing a means for price discovery and offsetting of price risks.

Quasi-Federal Government Organizations

The Financial and Banking Information Infrastructure Committee (FBIIC)

FBIIC is chartered under the President's Working Group on Financial Markets, and is charged with improving coordination and communication among financial regulators, enhancing the resiliency of the financial sector, and promoting the public/private partnership. The Treasury's assistant secretary for financial institutions chairs the committee.

In fulfilling its mission, the committee:

- Identifies critical infrastructure assets, their locations, potential vulnerabilities, and prioritizes their importance to the financial system of the U.S.;
- Establishes secure communications capability among the financial regulators and protocols for communicating during an emergency; and
- Ensures sufficient staff at each member agency with appropriate security clearances to handle classified information and to coordinate in the event of an emergency.

The Financial Services Sector Coordinating Council (FSSCC)

FSSCC is an organization comprised of representatives from financial services organizations and trade associations. This council fosters and coordinates sector-wide voluntary activities and initiatives designed to improve critical financial infrastructure and homeland security. The FBIIC and the FSSCC work closely with the U.S. Department of Treasury to combat financial crime, to strengthen the critical financial infrastructure of the U.S., and to mitigate the effect of manmade and natural disruptions on the financial system.

Objectives of the FSSCC:

- Identifying and reducing financial sector vulnerabilities by enhancing business continuity and contingency planning; business continuity mandates; expanding regional capabilities; and communicating critical information
- Ensuring the resilience of financial infrastructure
- Promoting public trust and confidence. Assuring that the public remains confident in the sector's ability to operate and to provide services to financial consumers will always be a key sector responsibility.

1.4 Mapping of Interdependencies

The security, economic prosperity, and way of life of the nation and its citizens depend on the reliable functioning of our increasingly complex and interdependent infrastructures. These include energy systems (electric power, oil, and natural gas), telecommunications, water supply

systems, transportation (road, rail, air, and water), banking and finance, and emergency and government services. Increasingly and at an accelerating pace, these interconnected infrastructures have become interdependent, increasingly fragile, and subject to disruptions that can have broad regional, national, and global consequences.

1.4.1 Upstream Sectors

The financial services sector is reliant not only on its own resources and infrastructures to support its businesses, but also on the telecommunications, energy and transportation sectors. Focus is on the dependency of the telecommunications sector. This became a focus of attention in 2004, with several groups taking action to explore this dependency in much greater detail and to develop recommendations on how sector members can address and minimize dependencies. Financial services companies recognize the complexity of the interdependencies they have with each other and with other sectors, and are establishing controls and policies to ensure adequate business continuity during periods of crisis. (Refer to appendix D for additional information on these sectors.)

Table 2: Upstream Sectors

Upstream Sectors	Banking and Finance Sector
Banking/Finance	
Emergency Services	
Energy	<ul style="list-style-type: none"> • Critical to this sector because of the need for electric power, diesel, and oil and gas to maintain operations and communication among firms and with the global networks of companies and the Internet. • The banking and finance sector infrastructure facilities depend upon electric power to function properly. The lack of power supply for the operation of computers/servers, air conditioners, etc., could be detrimental if out for a long period of time. For the short interval of power outage, most financial institutions depend on backup supplies of power, such as generators, however, if the outage is for a significant period, this situation can get serious if the financial institution has not stored enough diesel, oil and gas to run the generators.
Health	
Postal/Shipping	
Telecommunications	<ul style="list-style-type: none"> • Critical for maintaining financial services business because most rely upon telecom to maintain funds and order transfers of which there are billions per day. • Access to funds/cash could be an issue for technicians needing to get cash from ATM's for gas for their cars, local repairs, and purchases. • The sector specifically relies on computer networks and telecommunications systems to assure the availability of its services. The potential for disruption of these systems is an

	important concern. For example, the equity securities market remained closed for four business days following 9/11, not because any markets or market systems were inoperable, but because the telecommunications lines in lower Manhattan that connect key market participants were heavily damaged and could not be restored immediately. As a mitigation measure, financial institutions have made great strides to build redundancy and backup into their systems and operations.
Transportation	<ul style="list-style-type: none"> • Critical to maintain staffing and business continuity in times of emergency. • The transportation of diesel during an emergency. • The diversity and size of the transportation sector makes it vital to the economy and national security. Interdependencies exist between transportation and nearly every other sector of the economy. • Movement of financial documents (checks, etc.,). • \$1 trillion in remittances in United States Postal Services at any moment in time.
Water	

1.4.2 Downstream Sectors

All sectors require that the banking and financial sector be sufficiently resilient so that businesses, households and the government can function, during and in the aftermath, of a crisis.

Table 3: Downstream Sectors

Downstream Sectors	Banking and Finance Sector
Banking/Finance	
Emergency Services	<ul style="list-style-type: none"> • Required to support the evacuation of staff in times of emergency. • Replenishment of critical supplies during extended incidents • Emergency financial support to displaced persons and vulnerable populations.
Energy	
Health	Required to support the evacuation and care of staff in times of emergency.
Postal/Shipping	<p>Most communication is via telecom systems on satellite, the Internet or telephone, however, the postal and shipping sector is essential for</p> <ul style="list-style-type: none"> ○ The transportation of checks and other documents, <i>though Check 21 regulation may lessen this dependency.</i>
Telecommunications	
Transportation	
Water	Necessary to maintain business continuity because much of the

	business of banking and finance survives on human capital, computing and account maintenance, and telecom. For example, water is necessary for the cooling of computer rooms in core payment and clearing and settlement systems.
--	---

1.4.3 Sidestream Sectors

Table 4: Sidestream Sector

Sidestream Sector	Banking and Finance Sector
Government	The banking and finance sector has long been heavily government regulated and is therefore accustomed to working with government agencies to achieve long-term goals. This puts it in a unique position when it comes to side-stream sectors such as government agencies of a variety of sorts, e.g. the FBI.

1.4.4 Other Dependencies

So far, the transportation sector has been only peripherally considered by the sector. However, the events of 9/11 and the Northeast blackout in 2003, demonstrated how anemic transportation and evacuation plans in New York and Washington, D.C.; the blackout caused dangerous congestion on roadways and mass transit; and people unaware of street closings had no idea where to seek safety or shelter to wait until the crisis was over. It seems logical that if another blackout were to happen again, the situation would be little different than it was in 2001 and 2003.

2. State of Security Assessment

2.1 Awareness of value of CIP and CIVA/RM

The banking and finance sector government regulatory agencies and related organizations are confident that they have built resilience in the operations that are critical, such as building ways to communicate and operate with each other. FBIIC continues to identify vulnerabilities, conduct risk assessments and ensure resiliency e.g., arrangements have been made at back-up sites to have access to Telecommunication Service Priority. Individual banks are subject to implementing the guidelines provided in the FFIEC Information Technology Booklets and those by the FED, FDIC and OCC. Today, business continuity practices emphasize safety and soundness practices. A key role in promoting infrastructure protection throughout the sector is from FSSCC member organizations. In 2004, these organizations made extensive contributions to identifying and recommending approaches and tools to mitigating vulnerabilities in the sector. All financial companies go through an assessment evaluation by their primary regulators at least every 18 months.

2.2 *Availability of appropriate tools (open source or proprietary)*

Regulatory agencies enforce compliance when necessary. Regulators and financial institutions identify vulnerabilities and recommend solutions. Examples of detailed-specific guidance, checklists, questions, and standards are:

- The FFIEC Information Technology Booklets.
- The OCC Bulletins.
- Interagency Papers on Sound Practices issued by the FED, OCC, and SEC.

2.2.1 *Vulnerability assessments*

Based on the literature review and focus groups of banking and finance firms and regulators, in all cases, the federal regulatory agencies are responsible for oversight of financial service companies and are, under mandate, to keep the system informed, examined, and enforced with regard to issues of critical infrastructure protection. Furthermore, from the efforts of the regulatory agencies and quasi-governmental specialty groups for the banking and finance sector, there is no shortage of security and vulnerability assessment-related questions and protocols for the banking and finance sector in the NCR that may be relied on for the purposes of the CIVA. Much of these methods are described in the examination manuals of the federal and state regulators.

2.2.2 *Compliance-oriented policies and procedures*

The Federal Reserve Board, the Office of the Comptroller of the Currency and the Securities and Exchange Commission in 2003 published *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*.⁶ The paper identifies three new business continuity objectives that have special importance in the post-9/11 risk environment for all financial firms. It also identifies four sound practices to ensure the resilience of the U.S. financial system, focusing on minimizing the immediate systemic effects of a wide-scale disruption of critical financial markets.

Post-9/11 Business Continuity Objectives

During discussions about the lessons learned from 9/11, industry participants and others agreed that three business continuity objectives have special importance for all financial firms and the U.S. financial system as a whole:

1. Rapid recovery and timely resumption of critical operations following a wide-scale disruption;
2. Rapid recovery and timely resumption of critical operations following the loss or inaccessibility of staff in at least one major operating location; and
3. A high level of confidence, through ongoing use of robust testing, that critical internal and external continuity arrangements are effective and compatible.

Sound practices

The federal regulatory agencies identified four broad, sound practices for core clearing and settlement organizations and firms that play significant roles in critical financial markets.

The sound practices are based on long-standing principles of business continuity planning in which critical activities are identified, a business impact analysis is conducted, and plans are developed, implemented, and tested. Adoption of the sound practices will help protect the financial system from the risks of a wide-scale disruption and reduce the potential that key market participants will present systemic risk to one or more critical markets because primary and back-up processing facilities and staffs are located within the same geographic region.

1. Identify clearing and settlement activities in support of critical financial markets.
2. Determine appropriate recovery and resumption objectives for clearing and settlement activities in support of critical markets.
3. Maintain sufficient geographically dispersed resources to meet recovery and resumption objectives.
4. Test recovery and resumption arrangements, routinely used by companies.

Implementation of sound practices - cost effectiveness considerations:

As stated in the *Interagency Sound Practices Paper*, the federal regulatory agencies recognize the importance of cost-effective business continuity planning. The costs associated with implementing sound practices can vary substantially depending on the extent to which incremental improvements may be needed to address the risks of a wide-scale disruption. Some firms that play significant roles in critical markets may need to implement only relatively minor improvements to their back-up arrangements. Other firms may adopt a more robust technology or upgrade software applications in order to achieve recovery objectives identified by the sound practices. To mitigate the costs of these enhancements, firms will integrate them into the strategic planning process (e.g., coordinate with planned enhancements to facilities, information system components and architecture, and business processes).

Firms recognize that adoption and testing of the sound practices will help to reassure their counterparts and customers that they can rapidly regain their ability to clear and settle transactions in critical markets. Similarly, firms participating in the financial system would enjoy greater assurance that critical market participants will be able to withstand a wide-scale disruption and meet their payment and settlement obligations, thereby minimizing the potential for cascading fails and resulting systemic risk. Firms report that market forces clearly recognize the interdependent nature of the financial system, and customers and counterparts increasingly expect firms to demonstrate their ability to continue operations should a wide-scale disruption occur.

Implementation by core clearing and settlement organizations:

Core clearing and settlement organizations are required to continue their accelerated efforts to develop, approve, and implement plans that substantially achieve the sound practices. Plans should and do provide for back-up facilities that are well outside of the current synchronous range that can meet within-the-business-day recovery targets. On a case-by-case basis, core clearing and settlement organizations may be given additional time to synchronous range, so long as they take concrete, near-term steps that result in substantially improved resilience. The amount of flexibility will be measured against factors such as board of directors and senior management's commitment to approved budgets, and adherence to aggressive timetables and interim milestones. Plans should include measurable milestones to assess progress in achieving the sound practices.

Implementation by firms that play significant roles in critical markets:

Firms with significant roles in critical financial markets should develop, approve, and implement plans that call for substantial achievement of the sound practices as soon as practicable, but generally by 2008. In some cases, a firm may find it necessary to provide for a longer implementation period in light of its respective risk profile, level of resilience, and unique business circumstances. All plans should incorporate interim milestones against which progress can be measured and should provide for ongoing consideration of the costs and benefits of achieving greater geographic diversification of back-up facilities.

Role of senior management and boards of directors:

The agencies believe, and industry participants confirm, that incorporation of the post-9/11 business continuity objectives and sound practices discussed in this paper raise numerous short and long-term strategic issues that require continuing leadership and involvement by the most senior levels of management. These issues must be considered in light of a firm's dependencies on other market participants and the need to achieve a consistent level of resilience across firms. Boards of directors should review business continuity strategies to ensure that plans are consistent with overall business objectives, risk management strategies, and financial resources. Decisions about overall business continuity objectives should not be left to the discretion of individual business units.

Federal Reserve policy statement on payments system risk:⁷

Below is the core the federal policy statement specifically addressing "policies for private sector systems" e.g., multilateral settlement systems, scope and administration of the policy, and risk factors and risk-management measures.

"The use of multilateral settlement systems introduces the risk that a failure of one participant in the system to settle its obligations when due, could have credit or liquidity effects on participants that have not dealt with the defaulting participant."

Multilateral settlement may, in some cases, also have the effect of altering the underlying bilateral relationships that arise between institutions during the clearing and settlement process. As a result, the incentives for, or ability of, institutions to manage and limit risk exposures to other institutions, as required under Regulation F,⁸ may be reduced.

In addition, in some cases, there may be no timely or feasible alternative to settlement through the multilateral system in the event that the system fails to complete settlement, due, for example, to a participant default. These factors may create added risks to participants in certain multilateral settlement systems relative to other settlement methods. As a result, a number of multilateral settlement systems and their participants have implemented a variety of risk-management measures to control these risks.

Clearinghouses may generate systemic risks that could threaten the financial markets or the economy more broadly. The failure of a system to complete settlement when expected could generate unexpected credit losses or liquidity shortfalls that participants in the system are not able to absorb. Thus, the inability of one participant to meet its obligations within the system when due, could lead to the illiquidity or failure of other institutions. Further, the disruption of a

large number of payments and the resulting uncertainty could lead to broader effects on economic activity. In addition, as the Federal Reserve has established net debit caps and fees for daylight overdrafts, along with other risk management measures for its payment services, the potential exists for intraday credit risks to be shifted from the Federal Reserve to private, multilateral settlement arrangements, either domestically or in other countries that have inadequate risk controls.

Operational risks, such as those relating to the reliability and integrity of electronic data processing facilities used in the clearing and settlement process, are addressed in standard supervisory guidance for depository institutions and their service providers. Operational-risk factors include those that could hinder the timely completion of settlement or the timely resolution of a settlement disruption in a multilateral settlement system. For example, for a system that anticipates recasting settlement obligations in the event of a participant default, operational obstacles could make it difficult or impossible for participants to arrange settlement outside the system on a timely basis in the event of a settlement failure. As a result, those participants expecting to receive funds could face significant liquidity risk. In addition, in some cases, failure to complete settlement on a timely basis could change the rights of participants with respect to the underlying payments, creating potential credit or liquidity risks. For example, institutions that are unable either to return or to settle for checks presented to them on the same day may lose the right to return the checks for insufficient funds.

Further, certain risk-control procedures implemented by a particular system may themselves entail operational risks. The ability of a system to execute a recast of settlements, implement guarantee provisions, or access lines of credit may depend on the operational reliability of the system's facilities.”

FFIEC IT Booklets

The *FFIEC Business Continuity Planning* and *FFIEC Operations Booklets* (these are discussed in detail in Appendix C.) highlight the critical aspects of effective business continuity planning and specifically address reliance on telecommunications networks and telecommunications providers. The booklets recommend financial institutions, identify and document single points of failure in internal and external communications systems, and establish appropriate service level agreements (SLA) with telecommunications service providers.

SEC and CFTC Rules

The Securities and Exchange Commission, National Association of Securities Dealers and the New York Stock Exchange require NASD and NYSE members to create and maintain a written business continuity plan, identifying procedures relating to an emergency or significant business disruption. Plans are in place and periodically tested. Under the rules, member must develop a plan that addresses 10 specific elements for business continuity, including data backup and recovery, all mission critical systems, critical business constituent impact, and alternate communications between the firm and its employees, regulators and customers. In addition, the continuity plan must address how the member will ensure that customers have prompt access to their funds and securities if the firm is unable to continue in business. The SEC and the Commodities Futures Trading Commission developed policies and procedures for applying

National Security and Emergency Preparedness (NS/EP) telecommunications programs to key market utilities and market participants.

2.2.3 Risk management methods

Financial services institutions are expected to follow the FFIEC guidelines and ensure that settlement and clearing systems are backed up so that they can function in and after a time of crisis. Hence, they must ensure that the check cashing and clearance systems and network systems are functioning. During the “2003 blackout,” most had contingencies in place to take care of the most critical issues; nearly everyone could access money through electronic systems and through ATM’s located where there was backup power.

Financial institutions not only look at compliance issues, but business continuity issues as well. The agencies encourage financial institutions to conduct a business impact analysis, analyze gaps, and determine the costs to fill the gaps and whether it is necessary to do so. However, the regulatory agencies must leave to the management of these companies this task: they can not do it for them. The regulatory agencies have powers to enforce compliance, but they examine infrequently, usually once every 18 months, so that detection of noncompliance may be seriously delayed. In addition, resource allocation for the application of appropriate tools is uniform among banking and finance sector companies, adjusting for the criticality of the types of operations, and are extensive with constant monitoring by regulatory agencies and improvement plans in place.

2.3 Allocation of resources to CIVA/RM

As noted during both focus group meetings, the federal government and other regulatory agencies take the Homeland Security Presidential Directives (HSPD) very seriously. It is costly to implement and to build robust back up systems outside Washington, in regional centers and at Federal Reserve Banks. For example, the Office of the Comptroller of the Currency [Federal Preparedness Circular (FPC) 65, Federal Emergency Management Agency (FEMA) - OCC–FPC65–FEMA⁹], focused on 1) devolution and reconstitution, 2) transfer of authority seamlessly, 3) and restoration. The agencies have deemed it absolutely necessary to update continuity of operations on a consistent basis. Testing of the continuity of operations by the companies has proven to be a valuable tool. As a major element in testing, rehearsal can help clarify where plans break down or are not as effective as first thought.

The application of appropriate tools through resource allocation is dependent on the type of business risk under consideration. Banking and finance firms’ senior management need to ensure that there are sufficient resources employed in the organization to ultimately emphasize the goal, as established by the agencies and regulators, of not doing any harm to the financial system.

2.4 Extent of implementation of CIP measures

The regulators can set minimum standards for banking and finance companies to meet with regard to safety and soundness of operations and financial risks. What’s more, they can enforce these standards through various means, including increased capital requirements, fines and orders for management and board member expulsion. Furthermore, it is in the interest of financial institutions’ management and shareholders that they comply with these standards, so their customers and clients will not lose faith due to lack of services in time of crisis. Thus, it is expected that the overwhelming majority of banking and finance companies meet the minimum

standard as prescribed by the regulators, and many will normally go beyond these to meet the competition. Implementation of CIP measures is uniform among banking and finance sector companies and extensive with constant monitoring by regulatory agencies and improvement plans in place.

2.5 *Extent of evaluation of CIP effectiveness*

As mentioned in 2.4 above, the financial service company regulators evaluate the protection of the critical infrastructure of individual companies through their examination powers and can enforce the compliance of these institutions. Furthermore, the Federal Reserve System is constantly monitoring, on an intra-day basis, the functioning of the payments system. Based on the diligence of the regulators, there is ample reason to believe that there is sufficient evaluation of critical infrastructure protection effectiveness. The evidence is extensive when crises have occurred, for example Y2K preparations.

As noted from the focus group meetings, one important area of evaluation of CIP effectiveness that is profoundly lacking, is the relationship of the banking and finance companies with federal, state and local government bodies in charge of responding to an emergency, such as FEMA, local police, military, state and local transportation departments, etc. The same can be said for interrelationships of the banking and finance sector with telecommunications and energy companies. It is in this area that regulatory agencies cannot improve CIP effectiveness, but only recommend.

3. Risk Reduction Programs and Processes

3.1 *Risk Reduction Project and Investment Recommendations*

Tools and decision processes

Promote existing tools in the NCR as suggested in the following publications and studies discussed in the previous section:

- FFIEC IT Booklets.
- OCC Bulletins.
- U.S. Treasury Vulnerability Assessment Plan (National Strategy Compendium – Banking and Finance, May 2002).
- BITS IT Service Provider Framework and Expectations Matrix.
- BITS Key Risk Measurement Tool (*Kalkulator*).
- The Interagency Guidance on Sound Practices to Strengthen the Resilience of the U.S. Financial System.

3.1.1 *Tactical steps for immediate benefit on the ground*

- The sector should support the robust financial services/information sharing and analysis center activities within the NCR through private/public sector cooperation and coordination.
- The sector should provide more effective risk modeling to meet immediate NCR goals and objectives through private/public sector cooperation.
- The Department of Homeland Security should develop and implement credentialing program and processes for emergency response and restoration for the banking and finance sector.

3.1.2 Strategic steps for long-term benefit on the ground

- Through a public/private sector coordination organization such as ChicagoFIRST, develop a public confidence and trust program for the NCR.
- Banking and financial firms, with the help of their respective regulators, should develop an awareness and education program for financial services customers in the NCR.
- Federal, state and local government preparedness agencies should work with senior corporate managers and executives to support banking and finance sector security goals and objectives for the NCR.
- Address lack of coordination with upstream critical infrastructure service providers.

3.2 Risk reduction process improvements

3.2.1 Recommendations for enhancements in general guidelines and best practice compliance standards

The regulatory agencies, banking and finance sector trade associations, and private firms need to develop a single guideline document for companies to follow regarding critical infrastructure protection.

3.2.2 Recommendations for enhancements in risk management

Develop a regional approach, such as ChicagoFIRST model, to build cooperation among the banking and finance sector firms and their regulators, and with those critical to its business continuity and appropriate federal, state and local government agencies in the NCR.

3.3 Specific recommendations for governance at the sector-level

3.3.1 Incentives

Detail Corporate and Security Governance Expectations

For the banking and finance sector, corporate governance is not only the purview of management and the board of directors, but extends to the federal and state regulators, depending on the type of financial services firm (e.g., banking, investment banking, credit union, etc.). Consequently, the extensive role of regulatory agencies in the operations and, particularly, security governance is a main driver of security standards, rate of implementation, and strategic planning and compliance. The involvement in the safety and soundness of a financial services company by its regulators makes these firms unique compared to other private sectors' companies.

Several organizations, such as BITS/Financial Services Roundtable, the Business Roundtable, and the National Association of Corporate Directors, have contributed their expertise to development of regulatory standards for the protection of the critical infrastructure of the banking and finance sector. It remains the responsibility of the regulators, however, to jointly provide similar principles relating to security of their members.

The FFIEC member agencies expect institution management to implement controls across the institution to mitigate IT operations-related risk consistent with the nature and complexity of the institution's technology environment. By regulatory requirements, banking companies must adopt the FFIEC guidelines in order to meet the safety and soundness criteria of the banking regulators. From the perspective of critical infrastructure protection of the banking and finance sector, safety and soundness of the institutions is what must be achieved to ensure the protection of this vital industry. Institutions developing or reviewing their operational controls, procedures, standards, and processes, have a variety of third-party sources to draw on for additional guidance, including outside auditors, consulting firms, insurance companies, industry and trade groups, and other technology professionals. In addition, many national and international organizations have developed guidelines and best practices. These guidelines and best practices provide benchmarks institutions can use to develop sound practices. The following organizations are a sample of standard-setting groups:

- The National Institute of Standards and Technology (NIST)
- The International Organization for Standardization (ISO) Information technology
- The Information Systems Audit and Control Association (ISACA) – Control Objectives for Information Technology (COBIT)
- The Institute of Internal Auditors (IIA)
- The Committee of Sponsoring Organizations (COSO) of the Treadway Commission

3.3.2 Organization and management

Integrate those aspects of the American National Standard Institutes (ANSI) standards, and the National Fire Protection Association (NFPA) 1600¹⁰ for the NCR that are not already part of banking and finance regulation. The NFPA 1600 establishes a common set of criteria and terminology for preparedness, disaster management, emergency management, and business continuity programs.

Focus group recommendations:

- The sector should employ public/private partnerships for regional banking and finance infrastructure protection.
- The sector should coordinate inter-governmental relationships with full information and advice of the private/public sector partnership organization.
- The Department of Homeland Security should develop legislation and regulation, if needed, to facilitate regional coordination in the banking and finance sector.

3.4 Specific recommendations addressing dependencies

3.4.1 Intra-sectoral

Develop regional coalitions of banking and finance sector companies to work to better achieve a level of cooperation necessary to help ensure a level of safety during a time of crisis. This has been a hallmark of the financial services industry for centuries during looming financial crises. It needs to be developed for other types of crises.

3.4.2 Inter-sectoral

As noted in section 1.4.1 above, the critical non-financial sectors for the banking and finance sector are telecommunications, energy and transportation.

3.4.3 Regional

The development of regional coalitions for the banking and finance sector is imperative to providing much greater protection of the critical infrastructure of the financial services industry.

3.5 *Measuring Effectiveness*

Effectiveness can be best measured through the oversight process of the financial services federal and state regulators and the analysis by industry groups such as the Financial Services Roundtable, American Bankers Association, Independent Bankers Association, Conference of State Bank Supervisors, National Association of Insurance Commissioners, SEC, CFTC, and other such groups. In addition, Congress can have a role in periodically holding hearings on the state of CIP of this critical sector.

3.6 *Managing Continuous Improvement*

Managing and maintenance of continuous improvement can be achieved through the federal and state regulatory apparatus, oversight by Congress, and constant vigilance by the financial services trade associations making the issues of CIP for this sector evident to Congress and the regulators.

4. Conclusion

4.1 *Overarching Findings*

- Based on an extensive literature review, there is no single repository of literature on the vulnerability assessments (VA's) for the banking and financial sector. The federal regulatory agencies consistently have been responsible for oversight of financial service companies and are under mandate to keep the system informed, examined and enforced with regard to issues of critical infrastructure protection.
- In general, VA requirements depend on the kind of financial institution and the requirements of specific regulators— e.g., credit union examiners questions for business continuity or information security will be considerably different than examiners of large, global banking companies.
- There are a significant number of tools, questionnaires, and audit materials available. In some cases, the Federal Financial Institutions Examination Council (FFIEC) has provided a useful integrated VA management program, with assessment questions; in other cases, private sector and/or public-private partnerships have produced frameworks for the especially complex issues (e.g., outsourcing and telecom diversity).
- There is no shortage of security- and vulnerability assessment-related questions and protocols for the banking and finance sector in the National Capital Region (NCR) that may be relied

on for the purposes of Critical Infrastructure Vulnerability Assessment/Risk Management (CIVA/RM).

- One of the major problems within the financial services sector of the NCR identified by the focus groups is credentialing key NCR banking and finance personnel to access restricted areas to maintain or restore operations during and immediately after an emergency. A credentialing process for incidents and planned events, which would be of immediate benefit to the banking and finance sector, does not exist and is not planned.
- A regional approach, such as ChicagoFIRST model, is necessary to build cooperation among the banking and finance sector firms and their regulators and with those critical to its business continuity and appropriate federal, state and local government agencies in the NCR.
- One important area of evaluation of CIP effectiveness that is lacking is the relationship of the banking and finance companies with federal, state and local government bodies in charge of responding to an emergency, such as FEMA, local police, military, state and local transportation departments, etc. The same can be said for interrelationships of the banking and finance sector with telecommunications and energy companies. Regulatory agencies cannot improve CIP effectiveness, but only make recommendations.
- The banking and finance sector relies on several critical infrastructure industries for continuity of operations. The telecommunications, energy (electric power, oil and natural gas), transportation, and public safety services sectors are critical to the maintenance of business continuity of the financial services sector.
- The focus groups indicate that there is a need for tabletop exercises in the NCR and these should be done at the physical, cyber, regional and federal government levels. They also suggested that identification of duplication and gaps that need filling must be addressed.
- Testing is done at the local level and includes the energy, telecommunications, emergency services, and the federal and state regulators.

4.2 Challenges

As has been documented, for example, in the National Strategy and other homeland security strategy documents and studies, the financial services sector is essential to sustaining the economy of the United States. Accordingly, the entities and networks that constitute the U.S. financial system are among the critical infrastructure that face increasing threats from terrorist and other disruptions. Transactions involving trillions of dollars occur in the U.S. financial markets annually. Any significant disruption of these will have serious adverse national and global consequences for economic activity. After the large-scale impact on financial markets and market participants that resulted from the 9/11 attacks, law enforcement and other government organizations continuously report that key institutions and communications networks that support the financial markets have been specifically identified as targets.

As the GAO reports noted in February 2003 and September 2004, the government entities responsible for key financial market participants have begun to take actions to ensure that financial institutions are taking steps to minimize disruptions from terrorist attacks, but challenges remain.¹¹ Ensuring sufficient actions are taken by the private sector organizations that participate in the financial markets is also a challenge for securities firms and regulators and their ability to implement business continuity plans that would allow them to resume activities. These are private business decisions that have external consequences if key institutions are not prepared for crises and the severity of the debilitating effects.

Another challenge facing the banking and financial sector is implementing the strategy—developed by industry representatives, financial service industry regulators and under the sponsorship of the U.S. Department of the Treasury—that addresses needed efforts to identify, assess, and respond to regional and sector-wide threats. For example, the sector is expected to analyze its infrastructure’s strengths, interdependencies, and vulnerabilities and develop strategies for responses to events. Much, if not all of these activities, have been under the purview of the financial regulatory agencies that daily oversee financial services companies, including exchanges and transfer agents. To meet this challenge, regional public/private sector partnerships must be adopted to establish cooperation among private firms, government agencies responsible for recovery during crises and the private sector firms that the banking and financial sector relies upon to support its business continuity.

Areas for future investigation

The banking and finance sector team held two focus group meetings, and below are recommendations for future work that resulted from these meetings. Participants included federal and state financial service regulators and financial institutions (see appendix B for full list participants).

- Develop “good practices” for credentialing and recommend implementation in the NCR within a framework for coordination with the many jurisdictional entities.
- Adopt the ChicagoFIRST model for use in the NCR to guide the development of an organization to promote and conduct private/public sector partnership.
- Improve coordination and communication within the financial sector. Resiliency of banking and critical infrastructures is crucial at both the macro and micro level.
- Improve the resiliency of the sector to telecommunications failures, e.g., requiring that there is circuit diversity.
- Make terrorist watch-lists available to financial institutions.
- Clarify the mandate of the Department of Homeland Security (DHS) Office of the National Capital Region. Is it strategic, tactical and or operational?
- Need standards for response to chemical, biological, radiological and nuclear (CBRN) threats.
- DHS should coordinate and fund tabletop exercises in National Capital Region.
- Improve public trust and confidence by encouraging financial service firms to disclose to their customers and clients what they need to do in the case of an emergency and who and at which offices and ATM’s might be the most likely to be functional during and emergency.
- Execute a sector model for the NCR:
 - Develop a manual covering:
 - Existing sector emergency management plans
 - How to communicate among participants in the sector with other critical firms in other sectors
 - Perimeter access procedures with other critical infrastructures
 - Damage assessment criteria with other infrastructures
 - Delineate agency responsibilities for coordinating with other critical infrastructures
 - Private sector guidelines for cooperating with other critical infrastructures in times of crisis
 - Accelerate and publish preparations of recovery and restoration plans
 - Guidelines for operations during specific critical incidents

Appendix A: Methodology for Data Gathering and Analysis

There are three steps that were undertaken to gather and analyze information regarding the banking and financial services sector of the NCR. They are:

- An extensive review of the literature on the vulnerabilities, critical infrastructure and the preparedness of the banking and financial services sector to mitigate, withstand and recover from a serious terrorist attack or crises at the national and regional levels. Much of this literature is from the extensive rules, regulations and guidance of the financial services regulators in their roles in oversight of the safety and soundness of banking and financial firms and exchanges. It is discussed and summarized in the body of the report and a bibliography is in Appendix H.
- Two focus groups were formed to gain the insights of experts in the financial services sector in the National Capital Region. The first group was composed of individuals from the federal and state financial services regulators, banking and finance trade associations and some banking firms (refer to Appendix B for the list of participants). This group provided the necessary background to understand the extent to which the regulators could go in protecting the critical infrastructure of the banking and finance sector. It is extensive, but not complete. The second focus group consisted of banking and insurance firms and a presentation by the director of ChicagoFIRST, Brian Tishuk. This group focused on what firms believed are the weaknesses in the NCR that would be necessary to alleviate and substantially improve their individual and collective safety of the critical infrastructure. Furthermore, the firms also turned to what needed to be done and at what level to develop these programs. The presentation by ChicagoFIRST was integral to their strong and unanimous recommendation to pursue a public/private sector initiative that lead to regional organization modeled after ChicagoFIRST.
- An analytical review of the literature, review of the regulatory rules, regulations and guidance on risk mitigation in the banking and financial services sector and the results of the focus groups formed the basis of the conclusions and recommendations. In as much as the vulnerability assessment tools are those used uniformly by the banking and finance industry and reviewed by the regulators in a coordinated process, the strengths and weaknesses are uniform among companies. The greatest strength and weakness in these tools are that they are firm specific and only system-wide in the rules and regulations of the payments system. Accordingly, the report concludes that there needs to be established a regional public/private sector organization to promote coordination and cooperation among the financial service sector firms and the sectors that have been identified as those critical to the banking and financial services sector.

Appendix B: Focus Group Participants

Angela Desmond, Federal Reserve Board

Anthony Demangone, National Association of Federal Credit Unions

Ben Stafford, Zeichner Risk Analytics

Bobby Anderson, GEICO

Brian Tishuk, ChicagoFIRST – (Presenter)

Catherine Orr, Credit Union National Association

Chuck Madine, Federal Reserve Board

Doug Johnson, American Bankers Association/Financial Services Sector Coordinating Council

J.R. Hontz, Chevy Chase Bank

James Creel, George Mason University

Jay Golter, Federal Deposit Insurance Corporation

Jerry Brashear, George Mason University

Gerald Hanweck, George Mason University

Jim Devlin, Office of the Comptroller of the Currency

John McCarthy, George Mason University

Jordana Siegel, George Mason University

Juan Marulanda, Lafayette Federal Credit Union

Lee Zeichner, Zeichner Risk Analytics

Lisa Skalecki, Riggs Bank

Matt Dellon, Independent Community Bankers Association

Michael Jackson, Federal Deposit Insurance Corporation

Patricia Doe, Andrews Federal Credit Union

Rob Drozdowski, American Community Bankers

Robert Engebret, Office of Thrift Supervision

Rod Nydam, George Mason University

Steve Malphrus, Federal Reserve Board

Appendix C: Review of Open Source Vulnerability Assessment/Risk Management Tools, Procedures and Processes

Sector Specific Tools, Procedures and Processes

The foregoing are studies that have been suggested by the authors to apply to almost any industry and critical asset. This section reviews a number of studies that apply specifically to the banking and finance sector.

The banking and finance sector team reviewed a number of documents including the Federal Financial Institutions Examination Council (Council) FFIEC IT booklets, Treasury's Vulnerability Assessment Plan, FDIC's Risk Assessment Tools and Practices for Information Security, OCC Bulletins, Federal Reserve and Interagency guidelines for examiners and bank management and other guidance documents (refer to the bibliography in appendix E). However, no open-source vulnerability assessment tool was identified. These documents covered financial services infrastructure ranging from retail to wholesale services and incorporate standards and practices that the banking and finance sector can all agree are relevant and appropriate and would apply nationally and regionally. The review consisted of regulatory agency reviews and guidelines, federal regulation, administrative guidance to examiners and management, and public and private sector guidance such as BITS work in developing the Operational Risk Tool, and IT Service Provider Framework.

U.S Department of Treasury's VA Plan, Compendium of Supporting Documents to the National Strategy, May 2002

This document lays out a vulnerability assessment plan focusing on the large scale financial sector in the United States. The document was written in response to PDD 63. The assessment plan's methodology breaks down the entire financial sector into 5 categories, identifies key assets, identifies assets with high interdependency, and provides cost benefit analysis. This leads to a perpetual/cyclical assessment beginning with data collection, going on to an analytical phase, and ending in a change phase, before returning to the first stage. The document breaks down each stage into its essential parts in an attempt to provide a roadmap for vulnerability assessments on the macro scale.

Federal Financial Institutions Examination Council (FFIEC) Information Security Booklet - IT Examination Handbook, December 2002

This booklet provides extensive guidance to examiners and banking organizations on determining the level of security risks to the organization and evaluating the adequacy of the organization's risk management.

FFIEC Management Booklet - IT Examination Handbook, June 2004

This booklet provides guidance to examiners and financial institution management. The examination procedures in this booklet assist examiners in evaluating financial institution risk management processes to ensure effective information technology (IT) management.

FFIEC Operations Booklet - IT Examination Handbook, August 2004

This booklet provides guidance to examiners and financial institutions on risk management processes that promote sound and controlled operation of technology environments. Information is one of the most important assets of an institution, and information technology (IT) operations should process and store information in a timely, reliable, secure, and resilient manner. This booklet addresses IT operations in the context of tactical management and daily delivery of technology to capture, transmit, process, and store the information assets and support the business processes of the institution. The examination procedures contained in this booklet assist examiners in evaluating an institution's controls and risk management processes relative to the risks of technology systems and operations that reside in, or are connected to the institution.

FFIEC Business Continuity Planning Booklet - IT Examination Handbook, March 2004

This booklet provides guidance and examination procedures to assist examiners in evaluating financial institution and service provider risk management processes to ensure the availability of critical financial services. Effective business continuity planning establishes the basis for financial institutions to maintain and recover business processes when operations have been disrupted unexpectedly.

BITS Framework for Managing Technology Risk for IT Service Provider Relationships, November 2003

The financial services industry increasingly relies on information technology (IT) service providers ("Service Providers") to support the delivery of financial services. This shift in the delivery of financial services, coupled with the deployment of new and dynamic technologies, has resulted in heightened industry awareness and concern, accompanied by increased regulatory scrutiny of financial institution risk assessment and management of outsourced IT services. In response, the BITS IT Service Providers Working Group developed the *BITS Framework for Managing Technology Risk for IT Service Provider Relationships (Framework)* in 2001. While the original *Framework* provides an industry approach to outsourcing, additional regulatory and industry pressures and issues have since emerged. To address these changes, the Working Group has updated the *Framework* with further considerations for disaster recovery, security audits and assessments, vendor management and cross-border considerations.

Consistent with current regulatory guidance, the *Framework* recommendations are intended to be applied selectively based on a financial services company's risk-assessment results. In this way, the *Framework* should be used as a reference, stimulating firms to ask the right questions and complementing individual institutions' risk-management policies.

BITS IT Service Provider Expectations Matrix, January 2004

The BITS IT Service Provider Expectations Matrix was created to promote a common understanding among interested parties of the financial services industry's needs related to information technology practices, processes and controls. By providing financial institutions, service providers, and audit and assessment organizations with a comprehensive set of expectations, the Expectations Matrix helps financial services companies to identify risks and comply with regulatory requirements, as well as to eliminate gaps in the audit and assessment processes.

Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System, April 2003

The Federal Reserve Board (Board), the Office of the Comptroller of the Currency (OCC) and the Securities and Exchange Commission (SEC) published an *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System* (2003). The Federal Reserve Bank of New York also participated in drafting the paper. The paper identifies three new business continuity objectives that have special importance in the post-September 11 risk environment for all financial firms. The paper also identifies four sound practices to ensure the resilience of the U.S. financial system, which focus on minimizing the immediate systemic effects of a wide-scale disruption on critical financial markets. The agencies expect organizations that fall within the scope of this paper to adopt the sound practices within the specified implementation timeframes.

FDIC: Risk Assessment Tools and Practices for Information System Security, September 2004

This document provides financial institutions and examiners with background information and guidance on various risk assessment tools and practices related to information security. The document states that a comprehensive information security policy should outline a proactive and ongoing program incorporating three components:

- Prevention
- Detection
- Response

Prevention measures include sound security policies, well-designed system architecture, properly configured firewalls, and strong authentication programs. This paper discusses two additional prevention measures: vulnerability assessment tools and penetration analyses. Vulnerability assessment tools generally involve running scans on a system to proactively detect known vulnerabilities such as security flaws and bugs in software and hardware. These tools can also detect holes allowing unauthorized access to a network, or insiders to misuse the system. Penetration analysis involves an independent party (internal or external) testing an institution's information system security to identify (and possibly exploit) vulnerabilities in the system and surrounding processes. Using vulnerability assessment tools and performing regular penetration analyses will assist an institution in determining what security weaknesses exist in its information systems.

Detection measures involve analyzing available information to determine if an information system has been compromised, misused, or accessed by unauthorized individuals. Detection measures may be enhanced by the use of intrusion detection systems (IDSs) that act as a burglar alarm, alerting the bank or service provider to potential external break-ins or internal misuse of the system(s) being monitored.

Another key area involves preparing a response program to handle suspected intrusions and system misuse once they are detected. Institutions should have an effective incident response program outlined in a security policy that prioritizes incidents, discusses appropriate responses to incidents, and establishes reporting requirements.

BITS Key Risk Measurement Tool and Calculator¹² for Information Security Operational Risks, July 2004

Intended as a tool for financial managers to use in evaluating the risks to their information systems, the BITS Key Risk Measurement Tool investigates several types of operational risk, including: Internal and external fraud, employment practices and workplace safety, Clients products and business practices, damage to physical assets, business disruption and systems failure, execution delivery and process management.

The *Calculator* is intended for use by financial institutions to identify key information security risks that should be considered in broader enterprise-wide operational risk models. The *Calculator* provides an extensive, but not exhaustive, list of common information security threats, vulnerabilities and corresponding controls to mitigate risk. It also provides a method for scoring and prioritizing risks based on the likelihood of threat occurrence, the degree of control implementation, and the level of control effectiveness.

OCC 2000-14, May 2000: Infrastructure Threats - Intrusion Risks

This bulletin provides guidance to financial institutions on how to prevent, detect, and respond to intrusions into bank computer systems. Intrusions can originate either inside or outside of the bank and can result in a range of damaging outcomes, including the theft of confidential information, unauthorized transfer of funds, and damage to an institution's reputation.

The prevalence and risk of computer intrusions are increasing as information systems become more connected and interdependent and as banks make greater use of Internet banking services and other remote access devices.

Management can reduce a bank's risk exposure by adopting and regularly reviewing its risk assessment plan, risk mitigation controls, intrusion response policies and procedures, and testing processes. This bulletin provides guidance in each of these critical areas and also highlights information-sharing mechanisms banks can use to keep abreast of current attack techniques and potential vulnerabilities.

According to CERT/CC's 2004 E-Crime Watch survey conducted among security and law enforcement executives by CSO magazine in cooperation with the United States Secret Service and the Carnegie Mellon University Software Engineering Institute's CERT[®] Coordination Center, a significant number of organizations reported an increase in electronic crimes (e-crimes) and network, system or data intrusions. Forty-three percent (43%) of respondents report an increase in e-crimes and intrusions versus the previous year and 70% report at least one e-crime or intrusion was committed against their organization. Respondents say that e-crime cost their organizations approximately \$666 million in 2003. However, 30% of respondents report their organization experienced no e-crime or intrusions in the same period.¹³

OCC 99-9, March 1999: Infrastructure Threats from Cyber-Terrorists

The purpose of this bulletin is to identify and raise awareness of the threats and vulnerabilities created by cyber-terrorism to the financial services industry. The OCC defines Cyber-terrorism

as: "the use of computing resources against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives." These can be operations to disrupt, deny, corrupt, or destroy information resident in computers or available via computer networks. Cyber-terrorists can be an individual, a criminal organization, a dissident group or faction, or another country. Attacks can be generated internally or externally, and may be directly against a computer system, or focus on the supporting infrastructure (telecommunications, electricity, etc.).

OCC 98-3, February 1998: Technology Risk Management - Control of Risks associated with Technology - Guidance for Bankers and Examiners. This document provides guidance on how national banks should identify, measure, monitor, and control risks associated with the use of technology regardless of their source. The OCC will review technology-related risks together with all other risks to ensure that a bank's risk management is integrated and comprehensive. The guidance applies both to safety and soundness and bank information system concerns. All national banks should follow the guidance in their risk management efforts. The Summary of Key Points contains two main parts. The first outlines the primary risks related to bank use of technology and the second describes a risk management process for how a bank should manage these risks. The technology-related risk management process involves three essential elements. A bank should (1) plan for its use of technology, (2) decide how it will implement the technology, and (3) measure and monitor risk-taking. These elements are critical to any effective technology-related risk management process of a well-managed institution, regardless of size.

Review of Cross-Sector Specific Tools

1. Review of cross-sector tools

BITS Guide to Business-Critical Telecommunications Services, November 2004

It has been established above that telecommunications resiliency and its components—diversity, recoverability and redundancy—are critical to financial institutions, their customers and the U.S. economy. Events like 9/11 and the 2003 Northeast blackout, which affected key portions of the U.S. financial services industry, demonstrate the financial sector's dependence on the telecommunications sector and energy/power. The *BITS Guide to Business-Critical Telecommunications Services* (2004) provides financial institutions with best-at-the-time industry business practices for understanding and managing risks associated with essential telecommunications services.¹⁴ It is written as a guide to business managers, continuity planners and other risk managers—from CEOs to procurement experts—as they analyze risks, conduct due diligence, contract for telecommunications services and integrate evolving regulatory requirements into business continuity plans.

This document highlights key considerations and poses questions that business continuity planners and other risk managers should ask themselves and their service providers, taking into account regulatory requirements and changes in the marketplace. Each section of the document begins with a set of questions. These questions are a starting point for a rigorous examination of a financial institution's business continuity strategy for telecommunications needs and they serve as considerations in procuring adequate levels of service from telecommunications service providers. Answering these questions will help individual financial institutions achieve the

necessary levels of diversity, redundancy, and recoverability of critical telecommunications services.

U.S. Department of Commerce – Manual of Security Policies and Procedures – Appendix K, April 2003

This document lists physical security levels based primarily on the number of employees, uses of the facility, and the need for public access. It is intended for all types of business and is applicable to banking and finance firms and agencies. The manual notes that final assignment of a security level to a building will be adjusted based on threat intelligence, crime statistics, agency mission, etc. The manual identifies the following security areas against four security levels:

- Perimeter security
 - Parking: Control of facility parking, post signs and arrange towing for unauthorized vehicles, ID system and procedures for authorized parking, adequate lighting for parking areas, closed circuit television (CCTV) monitoring
- Entry Security
 - Receiving and shipping
 - Access control
 - Entrances and exits
- Interior Security
 - Employee and visitor identification
 - Utilities
 - Occupant emergency plans
 - Day care center
- Security Planning
 - Intelligence sharing
 - Training
 - Administrative procedures
 - Construction and renovation

Critical Infrastructure Assurance Office – Vulnerability Assessment Framework, October 1998

Homeland Security Presidential Directive / HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection, December 2003, directed Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks. Presidential Decision Directive 63 directed every department and agency of the Federal Government to develop a plan to protect its own critical infrastructure, including but not limited to its cyber-based systems. This directive applies to the federal financial regulators. It advises that consideration should be given to basing the plan on what is best suited to its mission and an identification of its critical infrastructures and their vulnerabilities, including:

- Identification of mission essential telecommunications, information, and other systems;
- Identification of significant vulnerabilities of the department's minimum essential systems; internal and external interdependencies; and

- An assessment of the vulnerability of the department's minimum essential services to failures by private sector providers of telecommunications, electrical power, and other infrastructure services.

The Vulnerability Assessment Framework (VAF) is designed to assist an agency's work on these issues. Based on existing security requirements and standards, the VAF can be applied across the federal government as well as to private sector infrastructures.

Through a three-step process, the VAF enables an organization to define its Minimum Essential Infrastructure (MEI), identify and locate interdependencies and vulnerabilities of its MEI, and provide the basis for developing its remediation plans.

Security Self Assessment Guide for IT Systems – NIST, August 2001

Adequate security of information and information processing systems are fundamental management responsibilities. Responsible officials are challenged to understand the current status of their organizations information security program and controls in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level.

This self-assessment guide utilizes an extensive questionnaire containing specific control objectives and techniques against which an unclassified system or group of interconnected systems can be tested and measured. The guide does not establish new security requirements. The control objectives and techniques are abstracted directly from long-standing requirements found in statute, policy, and guidance on security.

The Vulnerability Assessment and Mitigation Methodology - RAND, National Defense Research Institute, February 2004

Vulnerability assessment methodologies for information systems have been weakest in their ability to guide the evaluator through a determination of the critical vulnerabilities and to identify appropriate security mitigation techniques to consider for these vulnerabilities. The Vulnerability Assessment and Mitigation (VAM) methodology attempts to fill this gap, building on and expanding the earlier RAND methodology used to secure a system's minimum essential information infrastructure (MEII).

The VAM methodology uses a relatively comprehensive taxonomy of top-down attributes that lead to vulnerabilities, and it maps these vulnerability attributes to a relatively comprehensive list of mitigation approaches. The breadth of mitigation techniques includes not only the common and direct approaches normally thought of (which may not be under one's purview) but also the range of indirect approaches that can reduce risk. This approach helps the evaluator to think beyond known vulnerabilities and

ASME Risk Analysis and Management for Critical Asset Protection: General Guidance (To be made public in the fall of 2005)

This document provides guidance on approaches and methodologies for the following:

- 1) Analyzing risks associated with adversary attacks
- 2) Identifying and developing countermeasures and consequence-mitigation strategies to reduce risks

3) Evaluating countermeasures and consequence-mitigation strategies using benefit-cost and other methods to inform resource allocation decisions.

The guidance in this document is intended to be broadly applicable to all sectors and was prepared as a general, broad framework. Sector-specific guidance will be developed based on this document by adding sector-specific features and examples. The approaches and methodologies presented are general in nature and ASME recommends that they should therefore be used only by experienced risk-analysis practitioners and decision makers. Existing asset assessments or new asset assessments based on qualitative methods can be interpreted with this guidance. An accompanying “*Asset Application Handbook*” to this guidance document will assist new asset assessments. However, translation and calibration methods will need to be developed in respective sector-specific guidance efforts. It is expected that existing security vulnerability assessment methods should evolve over time toward a single standard.

This guideline is an approach to a standard and includes a listing of standard terminology with a definition for each term. Risk-analysis practitioners and other stakeholders use this terminology to ensure that risks are managed, mitigated, and communicated effectively. In order to provide the most structured basis for decision making, this document uses a “scenario-based” rather than an “asset-based” approach. Also, in order to provide a basis for comparison of risks across industry sectors and to provide meaningful input to the decision-making process, the risk-analysis methodology in this document is based on quantifying threat vulnerability, consequence, and risk to the extent practicable.

A screening methodology provided in the guideline offers the means to decide which assets may not require the more detailed risk analysis and which of them should be assessed further using the detailed approach in this document. The screening methodology does not employ quantification in most cases, but approaches are provided to quantify some aspects of the results, if necessary. It is intended that existing risk-analysis methods be used, but that they be modified as necessary to make them consistent with the methodology described in this guideline. It recognizes that, in most cases, the frequency or probability of a specific adversary action against a specific asset or target can be determined only within very broad ranges. However, if the best available data are used, together with appropriate models and expert opinion, the resulting ranges will bound the problem much more effectively and will provide a better basis for decision making and for the communication of risks, than simple qualitative estimates of high, moderate, or low.

Energy Infrastructure Vulnerability and Risk Assessment Checklists for State Governments, December 2001

Various approaches to the analytical risk management (ARM) process have been developed for various situations and a range of assessments. DOE has developed an initial checklist approach to the ARM process based on an established procedure for examining the security risk of a single facility or small-scale operation. However, the concepts presented should also apply to larger systems and to the overarching infrastructure, such as found within the various components of the energy infrastructure.

The checklist approach was developed for use by the participants in DOE’s November 2001 Initiative. It includes an overview of a fairly standard, top-level approach to concepts of vulnerability and risk assessments and lists of questions and considerations for use during each

major step of the risk management process. The purpose is to assist those state government officials who are tasked with identifying priorities for protecting the nation's energy infrastructure.

This checklist is designed for use by state and federal government officials who are:

- Reviewing vulnerability and risk assessments that have been conducted, especially those for which the reviewer was not a participant;
- Updating vulnerability and risk assessments (it is expected that users of the checklist would be active participants in the assessment process); and
- Conducting vulnerability and risk assessments (starting from scratch, again with users of the checklist as active participants in the assessment).
- Develop a list of current and potential concerns to head off surprise attacks.

The Electronic Intrusion Threat National Security and Emergency Preparedness (NS/EP) Internet Communications, National Communications System, December 2000

This report examines the electronic intrusion threat to national security and emergency preparedness (NS/EP) communications on the Internet. Electronic intrusion threat is an essential factor to be considered in risk assessments and as such, provides a baseline for countermeasure development. The analysis in this report is based exclusively on open source material. The techniques involved in computer intrusion and telecommunications and information systems targeting are described, and the motives of those who pursue such activities are discussed. The report also examines how attacks targeted at the Internet and related networks or which use the Internet as an attack medium may affect NS/EP communications networks.

The report raises awareness of the threats to NS/EP activities that rely on the Internet. A threat to information systems is defined as any circumstance or event with the potential to harm an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial or disruption of service. Electronic intrusion is examined in the context of the threat it poses to NS/EP communications, which rely on the Internet and the telecommunications and information systems to which the Internet is linked.

In addition, this report reviews the opportunities that intruders may be afforded by global interconnectivity and the availability of inexpensive and powerful technological capabilities, and discusses the implications of these trends for the increasing use of Internet systems for NS/EP communications. This report should raise awareness of the problem of global interconnectivity for the banking and finance sector.

Appendix D: Upstream and Downstream Sectors

Upstream Sectors

Telecommunications

The financial services sector is reliant not only on its own resources and infrastructures to support its businesses, but also on the telecommunications, energy and transportation sectors. We focus first on the dependency on the telecommunications sector. This became a focus of attention in 2004, with several groups taking action to explore this dependency in much greater detail and to develop recommendations on how sector members can address and minimize it. Financial services companies have come to recognize the complexity of the interdependencies they have with each other and with other sectors and are establishing controls and policies to ensure that adequate business continuity during periods of crisis.

In February 2002, the National Security Telecommunications Advisory Committee (NSTAC) and the National Communications System (NCS) released a report, *An Assessment of the Risk to the Security of the Public Network*, about the vulnerabilities of the telecommunications sector. This report concluded that “...(1) the vulnerability of the public network to electronic intrusion has increased, (2) government and industry organizations have worked diligently to improve protection measures, (3) the threat to the public network continues to grow as it becomes a more valuable target and the intruder community develops more sophisticated capabilities to launch attacks against it, and (4) continuing trends in law enforcement and legislation have increased the ability of the government and the private sector to deter the threat of intrusion.” The report also stated that the implementation of next-generation network technologies, including wireless technology, and their convergence with traditional networks, have introduced even more vulnerabilities into the public network.

Identifying “Best Practices”: In April 2004, a Financial Services Task Force of the NSTAC, published its *Financial Services Task Force Report* that provided a thorough review of these issues, and set forth findings and recommendations of value to sector member firms in addressing these issues.

Findings from this report included:

- Comprehensive business continuity planning and practices are essential.
- The Nation needs telecommunications networks that operate in a resilient manner.
- National Security and Emergency Preparedness functions should acquire the highest levels of telecommunications resiliency assurances available.
- Ensuring uncontaminated network resiliency and diversity is costly.
- A clear understanding between contracting parties is critical.
- Cross-sector understanding needs to be promoted.

Recommendations included:

- Support financial services sector initiatives examining:
- The development of a feasible “circuit by circuit” solution to ensure telecommunications services resiliency, and

- The benefits and complexities of aggregating sector-wide NS/EP telecommunications requirements into a common framework to protect national economic security.
- Coordinate and support relevant cross-sector activities (e.g., standards development, research and development, pilot initiatives, and exercises) in accordance with guidance provided in Homeland Security Presidential Directive 7.
- Provide statutory protection to remove liability and antitrust barriers to collaborative efforts is needed in the interest of national security.
- Continue to promote Telecommunications Service Priority program as a component of the business resumption plans of financial services institutions.
- Promote research and development efforts to increase the resiliency and the reliability of alternative transport technologies.
- Examine and develop capital investment recovery incentives for critical infrastructure owners, operators, and users that invest in resiliency mechanisms to support their most critical NS/EP telecommunications functions.

In September 2004, the Assuring Telecommunications Continuity Task Force of the Payments Risk Committee of the Federal Reserve Bank of New York published its *Best Practices to Assure Telecommunications Continuity for Financial Institutions and the Payment and Settlements Utilities*. Since financial markets are highly dependent on exceedingly complex telecommunications networks, the resiliency of these networks is crucial for the markets they serve and for the overall financial stability of the country. The report identifies thirteen Best Practices, outlined below.

- #1: Establish policies and procedures covering vendor services, staffing, documentation, and security to facilitate sound telecommunications administration.
- #2: Adopt Internet Protocol as the preferred telecommunications protocol.
- #3: Configure communications links for maximum physical diversity.
- #4: Regularly test backup facilities to ensure availability.
- #5: Use SONET (or equivalent “self-healing” technology) to connect data centers to carrier central offices to make connections as resilient as possible.
- #6: Consider the use of a variety of alternative technologies and services to address potential “last-mile” and inter-facility bottlenecks and single points of failure that cannot be resolved with conventional services.
- #7: Concentrate multiple circuits to fewer, higher bandwidth circuits in order to simplify connectivity and better assure diversity.
- #8: Adopt an “active-active” architecture where possible, with multiple mutually supporting active operational facilities and/or data centers.
- #9: Consider multiple carrier networks for provisioning of circuits.
- #10: Establish diversity criteria for carriers and develop audit programs to ensure compliance with the criteria.
- #11: Conduct regular audits of telecommunications documentation and diversity.

#12: Design frame relay networks to avoid Network-to-Network Interconnects (NNIs) and reduce complexity and single points of failure inherent with some NNI connections.

#13: Assign responsibility for circuit monitoring and the initiation of troubleshooting and repair of circuits connecting financial institutions and a payment and settlement utility to the utility.

Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System

The federal financial service regulators have developed a position on strengthening the resilience of the banking and financial system to vulnerabilities from sectors that are critical to the financial system. The Federal Reserve Board, Office of the Comptroller of the Currency and the Securities and Exchange Commission issued requirements in April 2003 for “core clearing and settlement organizations” and “financial institutions that play significant roles in critical markets,” in *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*. The paper acknowledges the effect telecommunications dependencies can have on recovery times.

Shortly after the September 11, 2001 attacks, the financial services industry, through BITS and other organizations, set out to mitigate unacceptable risks by engaging the telecommunications industry in dialogue on how best to assure sufficient levels of diversity, recoverability, redundancy and resiliency from its telecommunications service providers. This took place in the context of financial institutions reviewing their business continuity plans to reflect the heightened risks posed by terrorism and evolving regulatory requirements. The *BITS Guide to Business-Critical Telecommunications Services (November 2004)* is the culmination of this dialogue. Telecommunications resiliency and its components—diversity, recoverability and redundancy—are critical to financial institutions, their customers and the U.S. economy. Events like 9/11 and the 2003 Northeast blackout, which affected key portions of the U.S. financial services industry, demonstrate the financial sector’s dependence on the telecommunications sector.

The *BITS Guide to Business-Critical Telecommunications Services* provides the following observations and guidance. Prior to 9/11, many in the financial services industry assumed that:

- Circuit diversity is achieved through the use of multiple carriers.
- Switched services in general, such as frame relay, inherently provide resiliency.
- More circuits mean more resilience.
- The Internet is inherently less reliable than telecommunications services.
- Diversity can be ordered as a contracted service.
- Internet Protocol (IP)-based services are not inherently reliable.

Since 9/11, many in the financial services industry and government have learned that more realistic assumptions are:

- Circuit diversity cannot be assumed when ordered from two different carriers.
- Frame relay is shared among carriers and this raises concerns about diversity.
- Diversity remains an issue between the financial institution premises and the telecommunications point of presence (“last mile”).

- The Internet worked very well during 9/11 for messaging.
- Diversity must be engineered and means different things to different carriers and customers.
- More small circuits require more effort to monitor than a few larger ones.
- IP-based services can offer advantages.
- Means other than just diversity of redundant circuits can assure resiliency of the function they must support, such as Synchronous Optical Network (SONET) and proprietary service offerings.
- One can expect to pay more for telecommunications services that are specifically engineered (e.g., specialized versus standard contracting) to meet the resiliency needs of financial services companies.

To address risks in today's environment and to address regulatory requirements, financial institutions have been encouraged by regulators and industry experts to seek telecommunications providers that can offer:

- No single point of failure
- Resilient infrastructure
- Engineered diversity and methods for maintaining the engineered diversity over time
- Low end-to-end latency
- Services supporting high-bandwidth needs
- Remote, out-of-band, management and testability
- Comprehensive event monitoring and reporting
- Strong network security

The following recommendations for financial institutions have been made by BITS as essential for achieving telecommunications resiliency (note these recommendations can be applicable to other sectors):

- Know your mission-critical functions (and dependencies) and understand your acceptance of business risk.
- Know the extent to which your continuity of mission-critical business operations relies on the diversity, recoverability, redundancy and resiliency of your telecommunications requirements.
- Identify mission-critical services and functions that pose the highest risk to the institution if they are disrupted.
- Analyze and assess vulnerabilities and threats to mission-critical services. Threats exercise vulnerabilities and include natural disasters, malicious actions, cyber attacks and exploitation of single points of failure.
- Understand how specific diversity, recoverability, redundancy and resiliency requirements affect your institution's ability to continue operations.
- Understand that standard contracting with multiple telecommunications service providers alone may not provide the necessary diversity, recoverability, redundancy and resiliency.
- Establish a trusted relationship with your telecommunications service provider (or system integrators/managed service providers) by conducting the necessary due diligence and oversight to detailed service engineering and established documentation of service level agreements (SLA's), to assure requirements are clearly stated. Structure contracts to address these needs on a continuing basis, and include regular metrics.

- Take advantage, where eligible, of U.S. government-sponsored programs that permit the financial services sector to use recovery and response tools such as the Telecommunications Service Priority (TSP), Government Emergency Telecommunications Services (GETS) and Wireless Priority Services (WPS).
- Understand that emerging high diversity, recoverability, redundancy and resiliency services may cost more than standard services.
- Continue to assess emerging telecommunications and alternate transport technologies to determine whether they could provide services to further assure the necessary levels of diversity, recoverability, redundancy and resiliency are achieved.

Energy

NCR infrastructure systems have both internal and external dependencies, which means a failure of one part of one infrastructure system (e.g., power distribution) will reverberate both within the same system and into other systems (e.g., water supply). The banking and finance sector infrastructure facilities depend upon electric power to function properly. Alternatively they maintain back-up supplies of power, water or other inputs, but they are usually short-term supplies intended for non-catastrophic disruptions. The sector's firms are not able to backup the transportation or telecommunications systems if the energy sector fails or becomes impaired.

The Financial and Banking Information Infrastructure Committee (FBIIC) in response to the power outage of August 14 -15, 2003 and Hurricane Isabel in 2003 prepared a brief report that acknowledged that though the sector was quite prepared in handling both crisis it showed the heavy reliance on diesel and steam. Most institutions operated on backup generators. While the power outage obviously impacted financial institutions in affected areas, the financial system and its participants were largely able to complete their business. The outage caused financial institutions to switch over to back-up power at headquarters, operations facilities, and data centers during the period.

The NYSE was able to obtain a backup steam-generation boiler with the assistance of the New York City Office of Emergency Management (OEM). The NYSE exchange indicated that the utility steam system had never failed before, including during the massive power outages in the 1960s and 1970s and on 9/11. In view of the events during the August 2003 blackout, however, the American Stock Exchange (AMEX) will be working with the SEC to determine what additional measures should be taken to improve the resilience of the exchange's cooling capacity.

Electric power production requires water and water services in several different forms:

- Cooling Water – Water intake and outlet structures and pipelines from lakes, rivers and ponds for power plant cooling systems;
- Make-Up Water – On-site storage facilities and local water wells and supply pipelines;
- Water Service – Local water supply pipelines and services to all facilities where personnel work and/or equipment cooling is needed.

According to a GAO report GAO-03-173, Critical Infrastructure Protection, Efforts on the Financial Services Sector to Address Cyber Threats, January 2003, energy sector vulnerabilities have also been identified. For example, in October 1997, the President's Commission on CIP

reported on the physical vulnerabilities for electric power related to substations, generation facilities, and transmission lines. It further added that the widespread and increasing use of supervisory control and data acquisition (SCADA) systems for controlling energy systems increases the capability of seriously damaging and disrupting them by cyber means. In addition, the previously discussed Internet security threat report also concluded that companies in the energy industry, along with financial services and high-tech companies, experience the highest rate of overall attack activity. According to the study, power and energy firms received an average of 1,280 attacks per company, and 70 percent of them had at least one severe attack during the period studied.

Downstream Sectors

All sectors require that the banking and financial sector be sufficiently resilient such that business, household and government can carry on with their respective functions during and in the aftermath of a crisis.

Appendix E: 911 Recommendations Implementation Act: Private Sector Preparedness

SEC. 7803

It is the sense of Congress that the insurance industry and credit-rating agencies, where relevant, should carefully consider a company's compliance with standards for private sector disaster and emergency preparedness in assessing insurability and creditworthiness, to ensure that private sector investment in disaster and emergency preparedness is appropriately encouraged.

SEC. 7803. EMERGENCY SECURITIES RESPONSE ACT OF 2004.

(a) **SHORT TITLE-** This section may be cited as the 'Emergency Securities Response Act of 2004'.

(b) **EXTENSION OF EMERGENCY ORDER AUTHORITY OF THE SECURITIES AND EXCHANGE COMMISSION-**

(1) **EXTENSION OF AUTHORITY-** Section 12(k)(2) of the Securities Exchange Act of 1934 (15 U.S.C. 78l(k)(2)) is amended to read as follows:

(2) **EMERGENCY ORDERS-**

(A) **IN GENERAL-** The Commission, in an emergency, may by order summarily take such action to alter, supplement, suspend, or impose requirements or restrictions with respect to any matter or action subject to regulation by the Commission or a self-regulatory organization under the securities laws, as the Commission determines is necessary in the public interest and for the protection of investors--

(i) to maintain or restore fair and orderly securities markets (other than markets in exempted securities);

(ii) to ensure prompt, accurate, and safe clearance and settlement of transactions in securities (other than exempted securities); or

(iii) to reduce, eliminate, or prevent the substantial disruption by the emergency of--

(I) securities markets (other than markets in exempted securities), investment companies, or any other significant portion or segment of such markets; or

(II) the transmission or processing of securities transactions (other than transactions in exempted securities).

(B) **EFFECTIVE PERIOD-** An order of the Commission under this paragraph shall continue in effect for the period specified by the Commission, and may be extended. Except as provided in subparagraph (C), an order of the Commission under this paragraph may not continue in effect for more than 10 business days, including extensions.

(C) **EXTENSION-** An order of the Commission under this paragraph may be extended to continue in effect for more than 10 business days if, at the time of the extension, the Commission finds that the emergency still exists and determines that the continuation of the order beyond 10 business days is necessary in the public interest and for the protection of investors to attain an objective described in clause (i), (ii), or (iii) of subparagraph (A). In no event shall an order of the Commission under this paragraph continue in effect for more than 30 calendar days.

(D) **SECURITY FUTURES-** If the actions described in subparagraph (A) involve a security futures product, the Commission shall consult with and consider the views of the Commodity Futures Trading Commission.

(E) EXEMPTION- In exercising its authority under this paragraph, the Commission shall not be required to comply with the provisions of--

(i) section 19(c); or

(ii) section 553 of title 5, United States Code.'

(c) CONSULTATION; DEFINITION OF EMERGENCY- Section 12(k)(6) of the Securities Exchange Act of 1934 (15 U.S.C. 78l(k)(6)) is amended to read as follows:

(6) CONSULTATION- Prior to taking any action described in paragraph (1)(B), the Commission shall consult with and consider the views of the Secretary of the Treasury, the Board of Governors of the Federal Reserve System, and the Commodity Futures Trading Commission, unless such consultation is impracticable in light of the emergency.

(7) DEFINITIONS- For purposes of this subsection--

(A) the term 'emergency' means--

(i) a major market disturbance characterized by or constituting--

(I) sudden and excessive fluctuations of securities prices generally, or a substantial threat thereof, that threaten fair and orderly markets; or

(II) a substantial disruption of the safe or efficient operation of the national system for clearance and settlement of transactions in securities, or a substantial threat thereof; or

(ii) a major disturbance that substantially disrupts, or threatens to substantially disrupt--

(I) the functioning of securities markets, investment companies, or any other significant portion or segment of the securities markets; or

(II) the transmission or processing of securities transactions; and

(B) notwithstanding section 3(a)(47), the term 'securities laws' does not include the Public Utility Holding Company Act of 1935.'

(d) PARALLEL AUTHORITY OF THE SECRETARY OF THE TREASURY WITH RESPECT TO GOVERNMENT SECURITIES- Section 15C of the Securities Exchange Act of 1934 (15 U.S.C. 78o-5) is amended by adding at the end the following:

(h) EMERGENCY AUTHORITY- The Secretary may, by order, take any action with respect to a matter or action subject to regulation by the Secretary under this section, or the rules of the Secretary under this section, involving a government security or a market therein (or significant portion or segment of that market), that the Commission may take under section 12(k)(2) with respect to transactions in securities (other than exempted securities) or a market therein (or significant portion or segment of that market).'

(e) JOINT REPORT ON IMPLEMENTATION OF FINANCIAL SYSTEM RESILIENCE RECOMMENDATIONS-

(1) Report required- Not later than April 30, 2006, the Board of Governors of the Federal Reserve System, the Comptroller of the Currency, and the Securities and Exchange Commission shall prepare and submit to the Committee on Financial Services of the House of Representatives and the Committee on Banking, Housing, and Urban Affairs of the Senate a joint report on the efforts of the private sector to implement the Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System.

(2) Contents of report- The report required by paragraph (1) shall--

(A) examine the efforts to date of private sector financial services firms covered by the Interagency Paper to implement enhanced business continuity plans;

(B) examine the extent to which the implementation of such business continuity plans has been done in a geographically dispersed manner, including an analysis of the extent to which such firms have located their main and backup facilities in separate electrical networks, in different

watersheds, in independent transportation systems, and using separate telecommunications centers, and the cost and technological implications of further dispersal;

(C) examine the need to cover a larger range of private sector financial services firms that play significant roles in critical financial markets than those covered by the Interagency Paper; and

(D) recommend legislative and regulatory changes that will--

(i) expedite the effective implementation of the Interagency Paper by all covered financial services entities; and

(ii) optimize the effective implementation of business continuity planning by the financial services industry.

(3) Confidentiality- Any information provided to the Board of Governors of the Federal Reserve System, the Comptroller of the Currency, or the Securities and Exchange Commission for the purposes of the preparation and submission of the report required by paragraph (1) shall be treated as privileged and confidential. For purposes of section 552 of title 5, United States Code, this subsection shall be considered a statute described in subsection (b)(3)(B) of that section 552.

(4) Definition- As used in this subsection, the terms `Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System' and `Interagency Paper' mean the interagency paper prepared by the Board of Governors of the Federal Reserve System, the Comptroller of the Currency, and the Securities and Exchange Commission that was announced in the Federal Register on April 8, 2003.

Appendix F: Bibliography

- American Society of Mechanical Engineers (ASME), *Risk Analysis and Management for Critical Asset Protection: General Guidance*, (public version to be available in the fall of 2005).
- BITS *Guide to Business-Critical Telecommunications Services*, November 2004.
- BITS *Information Technology Service Provider Expectations Matrix*, January 2004.
- BITS *Framework for Managing Technology Risk for IT Service Provider Relationships*, November 2003.
- BITS *Key Risk Measurement Tool and Spreadsheet (Kcalculator) for Information Security Operational Risks*, July 2004.
- Critical Infrastructure Assurance Office, *Vulnerability Assessment Framework 1.1*, Oct. 1998.
- Department of Veterans Affairs (VA), *Physical Security Assessment for VA Facilities*, September 2002.
- Federal Deposit Insurance Corporation, *Risk Assessment Tools and Practices for Information System Security*, July 1999.
- Federal Financial Institutions Examination Council, *Information Security Booklet – IT Handbook*, December 2002.
- Federal Financial Institutions Examination Council, *Management Booklet – IT Handbook*, June 2004.
- Federal Financial Institutions Examination Council, *Operations Booklet – IT Handbook*, August 2004.
- Federal Financial Institutions Examination Council, *Business Continuity Planning Booklet – IT Handbook*, March 2003.
- Federal Reserve Bank of New York, *Best Practices to Assure Telecommunications Continuity for Financial Institutions and the Payment and Settlements Utilities*, September 2004.
- Federal Reserve System, Office of the Comptroller of the Currency, and the Securities and Exchange Commission, *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*, April 2003.
- Financial Services Sector Coordinating Council, *Statement on Telecommunications Resiliency*, September 2004.

General Accounting Office, *Critical Infrastructure Protection: Efforts of the Financial Services Sector to Address Cyber Threats*, January 2003.

Homeland Security Presidential Directive / HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection*, December 2003.

National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, February 2003.

NIST, *Security Self-Assessment Guide for IT Systems Questions/Guidance*, August 2001.

NIST, *Publication 800-26, Security Self Assessment Guide for Information Telecommunications Systems*.

NIST, 800-58, *Security Guidelines for VoIP systems*.

NIST, 800-34, *Contingency Planning Guide for Information Telecommunications Systems*.

NIST, 800-53, *Recommended Security Controls for Federal Information Systems*.

NSTAC *Financial Services Task Force Report*, April 2004.

NRIC, *Best Practices*, 2004, and all councils www.bell-labs.com/user/krauscher/nric/

Office of the Comptroller of the Currency, *2000-14: Infrastructure Threats – Intrusion Risks*, May 2000.

Office of the Comptroller of the Currency, *99-9: Infrastructure Threats from Cyber-Terrorists*, March 1999.

Office of the Comptroller of the Currency, *98-38: Technology Risk Management: PC Banking Description, Guidance for Bankers and Examiners*, May 2000.

Office of the Comptroller of the Currency, *98-3: Technology Risk Management – Control of Risks Associated with Technology*, February, 1998.

Presidential Decision Directive (PDD) 63: *Critical Infrastructure Protection*.
22 May 1998.

RAND's *Vulnerability Assessment and Mitigation Methodology*, February 2004: *Finding and Fixing Vulnerabilities in Information Systems*.

U.S. Department of Commerce, *Manual of Security Policies and Procedures*, April 2003.

U.S. Department of Energy, *Energy Infrastructure Vulnerability and Risk Assessment Checklists for State Governments*, December 2001.

U.S. Environmental Protection Agency, *Interim Voluntary Security Guidelines for Water Utilities*, December 2004.

U.S. Department of Treasury, *Vulnerability Assessment Plan: Compendium of Supporting Documents to the National Strategy* May 2002.

Appendix G: Definitions

Critical Infrastructures: Those systems and assets—physical and digital/cyber and human capital—so vital to the Nation that their disruption, incapacity or destruction would have a debilitating impact on national security, national economic security, and/or national public confidence, health and safety.¹⁵

Threat: A foreign or domestic entity possessing both the capability to exploit a critical infrastructure's vulnerabilities and the malicious intent of debilitating defense or economic security. A threat may be an individual, an organization, or a nation.¹⁶

Vulnerability: A characteristic of a critical infrastructure's design, implementation, or operation of that renders it susceptible to disruption, destruction or incapacitation by a threat.¹⁷

Vulnerability Assessment: Systematic examination of a critical infrastructure, the interconnected systems on which it relies, its information, or product to determine the adequacy of security measures, identify security deficiencies, evaluate security alternatives, and verify the adequacy of such measures after implementation.¹⁸

Appendix H: Acronyms

ANSI: American National Standards Institute
CBRN: Chemical, Biological, Radiological and Nuclear
CFTC: Commodities Futures Trading Commission
CIP: Critical Infrastructure Protection
CIVA/RM: Critical Infrastructure Vulnerability Assessment/Risk Management
COBIT: Control Objectives for Information Technology
COSO: Committee of Sponsoring Organizations of the Treadway Commission
DISB: Department of Insurance, Securities and Banking
FBI: Federal Bureau of Investigation
FBIIC: Financial and Banking Information Infrastructure Committee
FDIC: Federal Deposit Insurance Corporation
FEMA: Federal Emergency Management Agency
FFIEC: Federal Financial Institutions Examinations Council
FRB: Federal Reserve Board
FRS: Federal Reserve System
FS/ISAC: Financial Services Information Sharing and Analysis Center
FSSCC: Financial Services Sector Coordinating Council
GAO: Government Accountability Office
HSPD: Homeland Security Presidential Directives
IIA: Institute of Internal Auditors
ISACA: Information Systems Audit and Control Association
ISO: International Organization for Standardization
IT: Information Technology
NASD: National Association of Securities Dealers
NCR: National Capital Region
NCUA: National Credit Union Association
NIST: National Institute of Standards and Technology
NS/EP: National Security and Emergency Preparedness
NYSE: New York Stock Exchange
OCC: Office of the Comptroller of the Currency
OTS: Office of Thrift Supervision
SEC: Securities and Exchange Commission
VA: Vulnerability Assessment

Appendix I: Endnotes

¹ Title 10 USC Sec. 2674 (f) (2)

² Source: Defending America's Cyberspace – National Plan for Information Systems Protection, Version 1.0, 2000

³ Source: Board of Governors of the Federal Reserve System, *Federal Reserve statistical release*, Flow of Funds Accounts of the United States: Flows and Outstandings Fourth Quarter 2004 (Washington, D.C. March 10, 2005).

⁴ Source: FFIEC is composed of the Comptroller of the Currency, one FED Governor, the OTS Director, the FDIC Chairman, and the Chairman of the NCUA Board.

⁵ The FFIEC was established by Congress on March 10, 1979, pursuant to the title X of the Financial Institutions Regulatory and Interest Rate Control Act of 1978 (FIRA), Public Law 95-630.

⁶ Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System. Federal Reserve System [Docket No. R-1128]; Department of the Treasury Office of the Comptroller of the Currency [Docket No. 03-05]; Securities and Exchange Commission [Release No. 34-47638; File No. S7-32-02]. <http://www.sec.gov/news/studies/34-47638.htm>

⁷ Federal Reserve Policy Statement on Payments System Risk as amended effective September 22, 2004. For additional information www.federalreserve.gov/boarddocs/press/other/2004/20041126/default.htm

⁸ Regulation F, 12 CFR part 206) is issued by the Board of Governors of the Federal Reserve System (Board) under authority of section 23 of the Federal Reserve Act (12 U.S.C. 371b-2). <http://www.bankersonline.com/regs/206/206-1.html>

⁹ Federal Preparedness Circular (FPC) 65, Federal Emergency Management Agency (FEMA); Federal Executive Branch Continuity of Operations (COOP), July 1999

¹⁰ National Fire Protection Association (NFPA) 1600 Standard on Disaster/Emergency Management and Business Continuity Programs 2004 Edition

¹¹ See GAO Government Accounting Office, Financial Market Preparedness: Improvements Made, but More Action Needed to Prepare for Wide-Scale Disasters, [GAO-04-984](#) (Washington, D.C.: Sept. 27, 2004); Potential Terrorist Attacks: Additional Actions Needed to Better Prepare Critical Financial Market Participants, [GAO-03-251](#) (Washington, D.C.: Feb. 12, 2003); and Potential Terrorist Attacks: Additional Actions Needed to Better Prepare Critical Financial Market Participants, [GAO-03-414](#) (Washington, D.C.: Feb. 12, 2003).

¹² The *Kalculator* is intended for use by financial institutions to identify key information security risks that should be considered in broader enterprise-wide operational risk models. The *Kalculator* provides an extensive, but not exhaustive, list of common information security threats, vulnerabilities and corresponding controls to mitigate risk. It also offers a method for scoring and prioritizing risks based on the likelihood of threat occurrence, the degree of control implementation, and the level of control effectiveness.

¹³ Source: <http://www.cert.org/about/ecrime.html>

¹⁴ This document supplements the *BITS Framework for Managing technology Risk for IT Service Provider Relationships* ("Framework").

¹⁵ Source: Defending America's Cyberspace – National Plan for Information Systems Protection, Version 1.0, 2000

¹⁶ Source: Defending America's Cyberspace – National Plan for Information Systems Protection, Version 1.0, 2000

¹⁷ Source: Defending America's Cyberspace – National Plan for Information Systems Protection, Version 1.0, 2000

¹⁸ Source: Defending America's Cyberspace – National Plan for Information Systems Protection, Version 1.0, 2000

This Page Intentionally Blank