

CRS Report for Congress

Homeland Security: Banking and Financial Infrastructure Continuity

Updated March 16, 2004

William D. Jackson
Specialist in Financial Institutions
Government and Finance Division



**Prepared for Members and
Committees of Congress**



Homeland Security: Banking and Financial Infrastructure Continuity

Summary

The Department of Homeland Security (DHS) has many responsibilities for ensuring the continuity of the “real” economy: production, distribution, and consumption of public and private goods and services. Other agencies, however, have long had similar responsibilities for the “financial” sectors of the economy, which interact with the sectors DHS oversees pursuant to P.L. 107-296. DHS has some responsibilities for financial sectors through Treasury Department links. Financial agencies carry out recovery and security activities independently but also coordinately with DHS. For additional information on homeland security, please consult the CRS current legislative issue “Homeland Security,” on congressional web site [<http://www.crs.gov/products/browse/is-homelandsecurity.shtml>].

This report outlines recovery modes to mitigate disasters in financial markets that events have tested, and recovery arrangements. (Such disasters are of two kinds: inability to conduct transactions, and large losses of asset value.) Homeland security requires the financial institutions important in supporting and maintaining domestic and international commerce to take steps to safeguard their ability to carry out basic functions. The backbone of the financial economy—the payment system—comes through banks, and monetary policy affects them immediately. Other crucial intermediation functions come through a variety of financial companies, including brokers, exchanges, other secondary market facilities, and insurance companies. So, many regulators and trade associations need to be involved.

Regulators, especially the Federal Reserve, have set out best practice guidelines. The steps include business information technology protocols, physical security protocols, and plans for continuity of markets and participants considered critical for the nation’s transactions. An Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System, as a new regulation, will likely have positive consequences for the survivability of financial businesses. Controversies have arisen, e.g., some insurers believe that federal regulators have no authority to require them to take such steps, and some in New York are concerned that the area will lose jobs as facilities become necessarily dispersed. Costs of application remain of concern. Further governmental and public-private initiatives have sought to strengthen the resiliency of the financial system’s computers, in view of increasing cyberattacks.

The 107th Congress enacted legislation strengthening security for and of financial institutions and markets. Congressional interest in arrangements for safeguarding financial sectors. In the 108th Congress, H.R. 657, as passed by the House, would strengthen the Securities and Exchange Commission’s role in recovery and continuity of securities and related businesses. H.R. 2043 would address bank risks under terrorism, among other things. Hearings also examined financial security. Members may want to address financial sector arrangements in light of General Accounting Office concerns presented at the hearings. Should a financial emergency occur worse than in the blackout of August 2003, further oversight would be likely. This report will be updated as developments warrant.

Contents

Banking and Financial Institutions are Critical Infrastructure	1
The Role of DHS	2
Safety Net Measures in Place	3
Financial Risks	3
Operational/Security Risks	4
Safety and Continuity in Recent Experience	4
Last Decades of 1900s	4
Y2K Threat	5
2001	5
Blackout of 2003	6
Financial Business Continuity Proposals	6
Congressional	6
Regulatory	8
Executive	10
Private Sector	13
Conclusion: Convergence of Private and Public Practices for Financial Recovery and Continuity	15
List of Major Acronyms	15

Homeland Security: Banking and Financial Infrastructure Continuity

Banking and Financial Institutions are Critical Infrastructure

Financial institutions, not only banks and other depositories, but also securities dealers, insurers, and investment companies, are collectively a critical infrastructure element for the U.S. economy.¹ They are essential to the minimum operations of the nation.² Financial institutions operate as intermediaries—accepting funds from various sources and making them available as loans or investments to those who need them. The test of their collective operational effectiveness is how efficiently the financial system as a whole allocates resources among suppliers and users of funds to produce real goods and services. America has grown far beyond a bank-centered financial economy: financial value has largely become resident on computers as data rather than physical means of payment: an area of particular vulnerability.

Financial institutions face two categories of emergencies that could impair their functioning. The first is directly financial: danger of a sudden drop in the value of financial assets, whether originating domestically or elsewhere in the world, such that a global financial crisis might follow. The second is operational: failure of physical support structures that underlie the financial system. Either could disrupt the nation's ability to supply goods and services and alter the behavior of individuals in fear of the disruption (or fear of greater disruption). They could reduce the pace of economic activity, or at an extreme, cause an actual contraction of economic activity.

Financial regulators generally address the former set of problems through deposit insurance and other sources of liquidity to distressed institutions, safety and soundness regulation, and direct intervention. They address the latter, operational, set through remediation (as with the Y2K problem), redundancy, and other physical security. Under the worst case scenarios, the Federal Reserve (Fed) can relieve the

¹ CRS Report RL31556, *Critical Infrastructures: What Makes an Infrastructure Critical*, by John Moteff, Claudia Copeland, and John Fischer.

² Congress specified financial services as one critical physical and information infrastructure in P.L. 107-56, § 1016, Oct. 26, 2001, 115 Stat. 400. Banking and finance are reaffirmed as critical infrastructure similar to telecommunications, water, etc. in key executive branch documents: *The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets*, at web site [<http://www.whitehouse.gov/pcipb/physical.html>], *The National Strategy to Secure Cyberspace*, at web site [<http://www.whitehouse.gov/pcipb>], and "Homeland Security Presidential Directive/Hspd-7", at web site [<http://www.whitehouse.gov/news/releases/2003/12/print/20031217-5.html>].

economic effects of either set by acting as lender of last resort to supply liquidity to the financial system, employing monetary policy to expand domestic demand (as it did following the 9/11 terrorist attacks). In the Terrorism Risk Insurance Act of 2002 (TRIA), Congress expanded the Fed's ability to act as lender of last resort to the financial and real economies.³ Congress may also legislate direct federal assistance to protect the financial infrastructure. It has done so to prevent troubled entities such as Chrysler, the Farm Credit System, and New York City from defaulting, thus harming their lenders, and potentially causing failure in major parts of the financial system and the economy.⁴ Collapse of one prominent entity could evoke a contagion effect, in which sound financial institutions become viewed as weak — today's equivalent of a bank run, in which panicked customers withdraw funds from many entities, probably causing others to fail as well.

The Role of DHS

The Department of Homeland Security (DHS), created by the Homeland Security Act of 2002,⁵ has jurisdiction over functions previously assigned to 22 agencies with respect to certain communications, transportation, and computer (“cyber”) security. These are essential parts of the physical infrastructure upon which the financial system relies as a user. They are also parts of the electronic infrastructure of information storage, retrieval, and transmission. The heart of financial services is information that providers transform into useful forms, such as account balances at banks, securities price quotations, executions of purchase and sales of financial assets, and payments on contractual obligations such as loans.

Although networks of communication are vital to their work, financial services companies do not generally maintain communications and transportation networks, nor design software or manufacture hardware and carriage devices such as airplanes and trucks. Security of communication thus resides with sectors covered by DHS.⁶ Financial institutions and their regulators operate in a different environment than nonfinancial ones: they have been developing appropriate (sometimes different) security protocols within existing frameworks. As noted below, however, DHS interacts with Treasury Department bodies concerned with financial security. The need for combined cybersecurity for data and physical operations of financial businesses, interconnected via the Internet and otherwise, had received the attention of the former federal Critical Infrastructure Assurance Office.⁷ And the Treasury has agreed with DHS to assign an expert in financial services matters from Treasury to

³ P.L. 107-297, Title III, November 26, 2002.

⁴ CRS Report 89-290, *Financial Crises of the 1970s and 1980s: Causes, Developments, and Government Responses*, coordinated by William D. Jackson.

⁵ P.L. 107-296, November 25, 2002.

⁶ See “Administering the New Department of Homeland Security,” at web site [<http://www.congress.gov/erp/legissues/html/isdhs2.html>].

⁷ Marcia Kass, “Business Continuity, Solutions Integration Highlight Homeland Security Conference,” *BNA's Banking Report*, Dec. 16, 2002, p. 969.

Homeland Security. Eventually, experts from other financial regulators will be rotated into the new position.⁸

Safety Net Measures in Place

Financial Risks

Financial regulation includes deposit insurers, safety and soundness regulators throughout the financial sectors, and the Fed as lender of last resort and ultimate protector of the financial system. The Fed has long stood ready to provide liquidity to the banking system. The Federal Deposit Insurance Corporation (FDIC) protects depositors against failure of a bank or savings association. It helps guard against depositor panics that drain banks of their funds and create a severe liquidity crisis as they curtail lending, or call in loans to meet deposit withdrawals. Even a healthy depository institution, otherwise untouched by any cause of failure, would not long withstand a depositor panic. The FDIC brings order to the process of resolving such a financial failure. This agency has long had authority to prevent the failure of a bank it deems essential, which Congress supplemented in the 1980s and 1990s to allow even greater flexibility. The FDIC may borrow up to \$30 billion from the U.S. Treasury, if needed for rescue operations. Credit unions have similar arrangements with their Central Liquidity Facility and Share Insurance Fund.

Although the securities industry lacks a pool of emergency liquidity, securities firms may also borrow from the Fed if it allows them. Government protects individual securities accounts against operational losses — although not collapses of market value — through the federally-sponsored Securities Investor Protection Corporation. All states have guaranty funds to make good the obligations of their state-regulated insurance companies in case of insolvencies, although, again, no pool of liquidity exists for most of this industry nationally. TRIA provides a federal backstop for insurers willing to provide terrorism insurance.⁹ Congress intended this law to assure that such insurance remains available, while protecting providers against catastrophic payouts in case of terrorist attacks. This Act has had little effect since potentially insured parties do not seem to want to take on its high rates.

Other agencies bolster the national financial safety net by seeking to maintain confidence in other ways. A multiplicity of entities and processes are part of the ongoing safety net, although they do not necessarily assure liquidity or rescue of a financial failure. For many years, the securities industry and securities issuers have had overseers and programs designed to prevent against collapse of confidence originating within the system. The Securities and Exchange Commission (SEC), directly and through industry-based self-regulatory organizations such as stock exchanges, and accountancy standards, has sought transparency (“disclosure”) in

⁸ “Treasury Introduces Upgrades Designed To Help Safeguard Financial Service System,” *BNA’s Banking Report*, Dec. 8, 2003, p. 836.

⁹ CRS Report RS21444, *The Terrorism Risk Insurance Act of 2002*, by Carolyn Cobb; and, CRS Report RS21445, *Terrorism Insurance: The Marketplace After the Terrorism Risk Insurance Act of 2002*, by Carolyn Cobb.

financial practices, and trading in public securities, of businesses. The Sarbanes-Oxley Act of 2002¹⁰ sought further to restore investor confidence by strengthening accountability for Corporate America. Both the Federal Housing Finance Board and the Office of Housing Enterprise Oversight (OFHEO) regulate safety and transparency of important non-depository housing finance institutions. The Commodity Futures Trading Commission (CFTC) oversees organized markets on futures and similar contracts, through self-regulatory organizations.

Every state has one or more regulatory bodies responsible for state-chartered banks, credit unions, thrift institutions, and companies engaged in securities and futures operations. Although state-chartered depository institutions are subject to much federal regulation, the states alone primarily regulate insurance companies, finance companies, mortgage bankers, and the like. All 50 states oversee industry-funded guaranty funds to cover insolvencies in insurance companies, and some sponsor insurance for credit unions. Regulatory bodies for their respective industries are: Conference of State Bank Supervisors, National Association of Insurance Commissioners, and North American Securities Administrators Association.

Most important for the worst cases of financial disruption, the Fed can inject funds into the economy to maintain liquidity in the financial system. Its authority to lend to individual institutions allows it to support institutions that analysts characterize as “too-big-to-fail,” because their collapse would pose a systemic risk to the economy. The Fed has statutory authority to lend to businesses directly in “unusual or exigent circumstances,” which Congress strengthened in TRIA.

Operational/Security Risks

Safety and soundness regulators set guidelines and issue specific regulations for redundancy and security in physical systems and financial systems. They have long required banking institutions to consider operating (security) risks in contingency planning, and most now include risk of catastrophic disruptions such as occurred on 9/11. The securities industry is refining its protocols along similar lines. Insurance and other nondepository, non-securities financial businesses have not yet revealed so much planning for continuity this way. Although vital to the economy, they are not considered as critical: few would regard inability to process car loans, for example, as the root problem that failure to process checks and securities would be.

Safety and Continuity in Recent Experience

Last Decades of 1900s. Sudden drops in the value of financial assets have affected the U.S. financial system late in the 20th century, including the stock market’s crash in 1987, the savings and loan/banking collapse of 1989-1991, the Gulf War shock of 1991, and the Asian/Russian financial crises of 1997-1998. The Fed and other financial regulators took positive steps to alleviate the resulting difficulties, providing liquidity to the banking system, and therefore to the economy. They then planned steps that in hindsight might have cushioned against experienced collapses of value. Following the stock market plunge in 1987, the President’s Working Group

¹⁰ P.L. 107-204, July 30, 2002.

on Financial Markets¹¹ issued recommendations, many of which became practice. That group resurfaced after the late-1990s international disturbances that threatened the U.S. through just one investment fund: Long Term Capital Management. It examined problems that certain derivatives posed to the economy in 1999. Congress passed reforms of federal deposit insurance and banking regulators' authorities over practices threatening depository institutions generally in 1989 and 1991.¹² Agency powers of persuasion, and the Fed's ability to lend to distressed entities for short-term liquidity, reinforce formal regulations requiring time not available during crises.

Y2K Threat. More recently, the operational safety net, particularly that created to defend against computer problems feared for the year 2000, worked. The widely anticipated Y2K "millennium bug" was a software programming problem that could have caused failures in the infrastructure upon which the system relies. Public and private groups spent much effort to prevent widely-feared collapse of financial capabilities on January 1, 2000; they succeeded. Y2K came and went without serious incident in 2000, but the systematic backups and safeguards provided against it proved invaluable when the unthinkable happened the next year.

2001. With the September 2001 destruction of the World Trade Center, both problems—financial loss of asset values, and operational interruption — occurred simultaneously. The financial side of the response worked well, as the Fed provided the necessary liquidity to prevent panic. It injected \$80 billion, then more, into the banking system. It arranged international facilities to keep financial economies operating globally. The Fed and other central banks cut interest rates worldwide, to ease pressures on borrowers. Its stimulus may have exceeded \$300 billion.¹³

The SEC issued emergency rules encouraging buying in the stock market once it reopened. Trading recommenced rapidly, as the U.S. Treasury security market opened on September 13, and the equities market was in full operation by September 17. Physical infrastructure recoveries took a few days of heroic efforts (e.g., running new connections into Manhattan). Off-site record keeping, sharing of working space with displaced competitors, and increasing reliance on electronic tracing and communications systems by institutions outside the attack area, allowed for resumption of near-normal operations quickly. Nonetheless, regulators and industry groups made it known that financial firms would need new contingency plans and stress tests to protect against more extreme situations in the future. Many insurance companies ceased protecting against terrorist-related claims or raised premiums for such coverage sharply. Operators of high-profile commercial properties now often go without terrorism indemnity, since high prices still accompany federally-supported

¹¹ This Group consists of the Treasury, Fed, SEC, and CFTC.

¹² Financial Institutions Reform, Recovery, and Enforcement Act of 1989, P.L. 101-73, August. 9, 1989; Federal Deposit Insurance Corporation Improvement Act of 1991, P.L. 102-242, Dec. 19, 1991.

¹³ "Economic Repercussions: Overview," by Gail Makinen. In the *CRS Electronic Briefing Book on Terrorism*, at web site [<http://www.congress.gov/brbk/html/ebter110.html>].

coverage, as noted above. The government also provides insurance to domestic airlines under the Air Transportation Safety and System Stabilization Act.¹⁴

Blackout of 2003. Emergency response measures noted above helped reduce the financial market damages from a massive Aug. 14 power blackout in the northeastern United States and Canada. The Treasury Department received no reports of major disruptions or losses of financial data, in large part because of steps taken to make systems resilient and redundant. Despite glitches, the major markets, in stocks, options, commodities, futures, and bonds, were soon open. Banks closed affected offices, in New York and Detroit; otherwise, the banking system overwhelmingly stayed open. The Fed's payments and emergency lending to banks systems operated well. Banks borrowed \$785 million from the Fed after the blackout, the most since \$11.7 billion of the week after Sept. 11, 2001, and have since repaid these amounts. New applications for mortgages did fall temporarily because of the blackout. Contrary to initial fears, terrorists had not caused the blackout and thus it did not severely stress the financial economy.¹⁵

Financial Business Continuity Proposals

The payments system continued to function after the attack on New York's financial activity. Providers realize that making their "primary site" coordinated with a "backup site" is not enough. Hardware and software differences between sites need to be resolved, for example. The banking sector now functions normally and, with increasing concerns over safety, has seen inflows of deposits and high profit—even while lending has experienced problems. Bond markets had recovered their trading levels, despite destruction of a company responsible for much of the market for government bonds. Bond prices, mirroring the downward movement in interest rates, are generally higher than in 2001 but are experiencing fears over their quality. The stock markets have recovered to a large degree. With the federal backstop for insurers, coverage of acts of terrorism has become available. Nonetheless, financial sectors remain cautious although optimistic.

Congressional

Legislation. The 107th Congress passed legislation to backstop terrorism insurance for property-casualty insurers and airlines. Application of such aid continues. Other congressional measures, including tax relief for investors and financial integrity initiatives, seemingly increased confidence in the securities markets by 2003. The House approved a bill to give the SEC additional authority in case of a national emergency, on February 26, 2003. This Emergency Securities Response Act, H.R. 657, introduced by Representative Garrett, would allow the SEC to extend emergency orders beyond the ten business days currently allowed. It also

¹⁴ P.L. 107-042, September 22, 2001.

¹⁵ "Measures Prompted by Sept. 11 Helped Banks Weather Electrical Outage, Snow Says," *BNA's Banking Report*, August 25, 2003, p.254; Todd Davenport, "In Brief: Outage Sparked \$785M of Fed Lending," *American Banker Online*, Aug. 22, 2003; and, Rob Blackwell, "Backup Site Questions, Utility Loan Prospects," *Ibid.*, August 18, 2003.

would expand the agency's ability to grant exemptions from federal securities laws. Emergency powers could extend for any period specified by the Commission up to 90 calendar days. The House approved a similar bill in 2001, which the Senate did not consider. The Senate has not taken up this year's measure either.

Oversight and GAO. The General Accounting Office (GAO) has reviewed threat mitigation in financial markets. GAO released two studies of continuity plans, physical security, and electronic security for exchanges, electronic communications networks, market support organizations, broker-dealers, banks, etc.

In the first, GAO recommended that the Treasury Department coordinate with the banking and finance industry in updating the sector's National Strategy for Critical Infrastructure Assurance and to fix interim objectives, detailed tasks, time frames, and responsibilities for the strategy and a process for monitoring its progress. To help these objectives, GAO suggested Treasury assess the need for grants, tax incentives, regulation, or other public policy tools.¹⁶ GAO also found deficiencies in the key Treasury/Federal Reserve internet payments system known as "pay.gov," which seem to have been fixed.¹⁷

Congress examined the agency's second set of findings¹⁸ in a House Financial Services Subcommittee on Capital Markets, Insurance and Government Sponsored Enterprises hearing held Feb. 12, 2003.¹⁹ GAO found that the Fed; the regulator of national banks, the Office of the Comptroller of the Currency (OCC); and SEC lack a strategy for having their regulatees resuming trading in securities following any future disruption of the financial market, and should work with industry to develop a plan. GAO's most direct recommendation for actions were primarily for the SEC's operations risk oversight. For bank regulation, GAO noted that examiners review physical security, but do not generally focus on terrorism mitigation.

¹⁶ U.S. General Accounting Office. *Critical Infrastructure Protection: Efforts of the Financial Services Sector to Address Cyber Threats*, GAO-03-173, January 30, 2003, at web site [<http://www.gao.gov>].

¹⁷ U.S. General Accounting Office. *Information Security: Computer Controls over Key Treasury Internet Payment System*, GAO-03-837, July 30, 2003, at web site [<http://www.gao.gov>].

¹⁸ It is available in three versions. U.S. General Accounting Office. *Potential Terrorist Attacks: Additional Actions Needed to Better Prepare Critical Financial Market Participants*. GAO03-251, *Potential Terrorist Attacks: Additional Actions Needed to Better Prepare Critical Financial Market Participants*. GAO03-414, and, *Potential Terrorist Attacks: More Actions Needed to Better Prepare Critical Financial Markets*, GAO03468T, all dated February 12, 2003, through web site [<http://www.gao.gov>].

¹⁹ "Recovery and Renewal: Protecting the Capital Markets Against Terrorism," at web site [<http://financialservices.house.gov/hearings.asp?formmode=detail&hearing=176>]

In a surprising finding, GAO's study of the Treasury's own information technology) protocols found that the Department's chief information officer needed to improve Department-wide financial information security controls.²⁰

Regulatory

Government Securities Clearing. Regulators are concerned about the U.S. government securities market, in view of its critical role for conducting monetary policy operations, financing government activities, and providing benchmark prices and hedging opportunities for other securities markets. On May 13, 2002, the Fed, the OCC, and the SEC issued a White Paper on Structural Change in the Settlement of Government Securities. That Paper expressed concerns about operational, financial, and structural vulnerabilities from having only two clearing banks for settling trades and financing positions. In response, the Fed announced it will explore a back-up "dormant" clearing and settlement bank, ready should the two banks clearing Government securities be unable to do so, as well as other mitigatory measures.²¹ One of them experienced a massive computer failure preventing this market from functioning two decades ago.²²

Communications. At the intersection of financial and communications markets, the Fed (in coordination with Treasury and the other banking agencies) has strengthened its programs for giving financial businesses emergency preparedness access to priority communications.²³ These programs, which the National Communications System administers, help financial markets facing substantial operational disruptions. They are: (1) Telecommunications Service Priority for circuits used in large-value interbank funds transfer, securities bidding and transfer, and payment-related services; (2) Government Emergency Telecommunications Service for priority processing of calls over terrestrial public switched networks; and (3) Wireless Priority Service of cellular calls during severe network congestion.

Interagency Paper on Sound Practices. The Fed, the OCC, and the SEC have issued an "Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System."²⁴ This final regulation²⁵ builds upon a draft from the

²⁰ U.S. General Accounting Office. *Improvements Needed in Treasury's Security Management Program*. GAO-04-77, through web site [<http://www.gao.gov>].

²¹ Federal Reserve Press Release, Jan. 30, 2004, at web site [<http://www.federalreserve.gov/boarddocs/press/other/2004/20040130/default.htm>].

²² U.S. Congress. House. Committee on Banking, Finance, and Urban Affairs. Subcommittee on Domestic Monetary Policy. *The Federal Reserve Bank of New York Discount Window Advance of \$22.6 billion Extended to the Bank of New York*, Washington: U.S. Govt. Print. Off., 1986. 575 p.

²³ Documentation of the policy, as sent to national banks, appears at web site [<http://www.occ.treas.gov/ftp/bulletin/2003-13.txt>].

²⁴ *Federal Register*, vol. 68, no. 70, April 11, 2003, pp. 17809-17814.

²⁵ At web site [<http://www.occ.treas.gov/ftp/bulletin/2003-14.txt>].

previous September.²⁶ The Interagency Paper, which applies most directly to the clearing and settlement activities of a few financial institutions, provides some flexibility to firms in managing geographic dispersion of backup facilities and staffing arrangements, and takes into account cost-effective application of sound practices. It includes participation from the New York State Banking Department and the Federal Reserve Bank of New York.

The Interagency Paper analyzes concerns of systemic risk: a breakdown in a transfer system or a financial market that cannot fulfill its obligations, creating liquidity and credit problems for customers. It focuses on protections for “core” check clearing and settlement and for financial companies involved in “critical markets,” such as federal funds, foreign exchange, commercial paper, and government, corporate, and mortgage-backed securities. This regulation deals with substantial interruptions of transportation, telecommunications, or power systems throughout a major region, perhaps with evacuation of population. It sets forth four broad sound practices that a covered firm should carry out:

- Identify clearing and settlement activities supporting critical financial markets;
- Determine appropriate recovery and resumption objectives for clearing and settlement activities in support of critical markets;
- Maintain sufficiently geographically dispersed resources to meet recovery and resumption activities, and;
- Routinely use or test recovery and resumption arrangements.

This paper suggests that practices for recovery and continuity include “robust” backup facilities for clearance and settlement activities, resumption of normal business within two hours, regular testing of backup facilities, and backup personnel. Issuing agencies stressed that it will take several years to carry out recommended sound practices fully. They did not recommend moving primary offices of financial and securities firms, contrary to some expectations.

The Interagency Paper does not cover most of the world of finance, however. It does not address retail or trading operations, nor the insurance sector. Since it only covers the largest entities of a wholesale nature, no other regulators issued it.

FFIEC. The four bank and single credit union regulatory agencies, however, meet together as the Federal Financial Institutions Examination Council. This Council’s information technology subcommittee serves as a vehicle for coordinating agency policies on technological and related risks now including security protocols and financial business continuity.²⁷ It is coming to have a larger role in physical- and cyber-security financial protocols.

²⁶ Federal Reserve System, Department of the Treasury, and Securities and Exchange Commission, “Draft Interagency White Paper on Sound Practices to Strengthen the Resilience of the U. S. Financial System,” *Federal Register*, vol. 67, no. 172, Sep. 5, 2002, pp. 56835-56842.

²⁷ Rob Blackwell, “Regulators Put Examiner Update Online,” *American Banker Online*, Jan. 30, 2003.

Basel II. For the largest U.S. commercial banking organizations, the Fed has proposed additional mandates in its planned regulation known as the "Basel II Capital Accord." Among the issues raised by Basel II is its controversial operational risk requirement for covered firms to carry greater capital. Operational risk refers to noncredit risk factors including system failures and terrorism, such as 9/11. Hearings by two subcommittees of the House Financial Services Committee in 2003 explored some of its implications, which most bankers feel are burdensome.²⁸ The 108th Congress measure, United States Financial Policy Committee for Fair Capital Standards Act, H.R. 2043, would address perceived needs to improve Basel II, including its operational risk component.

Fed Rescue Plan. In the broader picture, the Fed is reportedly planning to lend massively to banks and other entities to ensure that financial markets do not lock up, should another major shock occur against the financial system. It may attempt such a rescue plan for the economy — even without another 9/11 emergency.²⁹

Executive

Government's Own Financing. Congress generally requires financial bodies within government itself to develop, document, and carry out agency-wide information security programs under the E-Government Act of 2002.³⁰ The Treasury Department and other federal bodies have taken steps to protect the government's critical financial functions including to: borrow; make payments including social security; and raise revenue through the Internal Revenue Service. Should the threat level rise, agencies will (1) increase physical and cyber-security measures including security forces, the frequency of security patrols, identity checks, and restricting access with state and local authorities to enhance physical security for specific assets; (2) disperse individuals critical to operations; and (3) use backup facilities.³¹

Presidential. President Bush has appointed executives of the banking and securities industries to the National Infrastructure Advisory Council (NIAC). The members of this panel advise the White House on cyber- and information-security of critical economic infrastructures, including financial ones. It builds upon, in part, the former Critical Infrastructure Assurance Office created in 1998 to coordinate federal initiatives on critical infrastructures. Members of NIAC represent major sectors of the economy — banking and finance, transportation, energy, information technology, and manufacturing. It also includes representatives from academia, state

²⁸ "The New Basel Accord — Sound Regulation or Crushing Complexity?" at web site [<http://financialservices.house.gov/hearings.asp?formmode=detail&hearing=182>], and, "The New Basel Accord — in Search of a Unified U.S. Position," at web site [<http://financialservices.house.gov/hearings.asp?formmode=detail&hearing=236>].

²⁹ "Fed Piecing Together Emergency Economy Plan," *Wall Street Journal Online*, April 7, 2003; and, "Fed Ferguson Says Emergency Econ Rescue Plan Exaggerated," *Ibid.*, April 8, 2003.

³⁰ P.L. 107-347, December 17, 2002.

³¹ "Treasury Statement on Measures to Protect the Financial Markets during Hostilities with Iraq," March 17, 2003, at web site [<http://www.treas.gov/press/releases/js114.htm>].

and local government, and law enforcement. NIAC works closely with the President's National Security and Telecommunications Advisory Committee.³²

NIAC meets periodically to:

(i) enhance the partnership of the public and private sectors in protecting information systems for critical infrastructures and provide reports to the Secretary of Homeland Security;

(ii) encourage private industry to perform periodic risk assessments of critical information and telecommunications systems;

(iii) monitor the development of private sector Information Sharing and Analysis Centers (ISACs) and provide recommendations to the President through the Secretary of Homeland Security on how these organizations can foster cooperation among ISACs, DHS, and other government entities;

(iv) report to the President through the Secretary of Homeland Security, who coordinates with the Assistant to the President for Homeland Security, the Assistant to the President for Economic Policy, and the Assistant to the President for National Security Affairs; and

(v) advise lead agencies with critical infrastructure responsibilities, sector coordinators, DHS, and ISACs, including for the banking and finance sector.³³

FBIIC. Treasury's Office of Critical Infrastructure Protection, formed after 9/11 under Treasury's Office of Financial Institutions, staffs the Financial and Banking Information Infrastructure Committee (FBIIC). Its chair is the Treasury's Assistant Secretary for Financial Institutions.³⁴ Its mission involves coordinating federal and state efforts to improve the reliability and security of the financial system.³⁵ FBIIC, created by Executive Order in 2001, includes representatives of the:

- Commodity Futures Trading Commission,
- Conference of State Bank Supervisors
- Department of the Treasury
- Federal Deposit Insurance Corporation
- Federal Housing Finance Board
- Federal Reserve Bank of New York
- Federal Reserve Board
- Homeland Security Council
- National Association of Insurance Commissioners
- National Credit Union Administration
- Office of the Comptroller of the Currency

³² "Appointments to National Infrastructure Advisory Committee," at web site [<http://www.whitehouse.gov/news/releases/2002/09/20020918-12.html>].

³³ "Executive Order Amendment of Executive Orders, and Other Actions, in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security," at web site [<http://www.whitehouse.gov/news/releases/2003/02/20030228-8.html>].

³⁴ It was the Office of Homeland Security's Financial Markets Work Group.

³⁵ Financial and Banking Information Infrastructure Committee, "FBIIC," at web site [<http://www.fbiic.gov>].

- Office of Federal Housing Enterprise Oversight
- Office of Thrift Supervision
- Securities and Exchange Commission.

In fulfilling its mission, FBIIC is to: (1) identify critical infrastructure assets, their locations, potential vulnerabilities, and rank their importance to the financial system of the United States; (2) secure communications capability between the financial regulators and protocols for communicating during an emergency; and (3) ensure sufficient staff at each member agency with appropriate security clearances to handle classified information and coordinate in case of an emergency. FBIIC will conduct vulnerability assessments of the retail payment system, government-sponsored enterprises, and the insurance industry — none directly addressed in the White Paper noted above — and other improvements to financial resiliency.³⁶ Along these lines, the Treasury has formulated new procedures for secure communications between federal and state financial regulators to share information about the impact of an event on the financial institutions that the regulators supervise.³⁷

Public/Private Treasury Efforts. Treasury has created a public/private partnership to ally with FBIIC, drawing together industry initiatives and coordinating private sector outreach for critical infrastructure protection and homeland security.³⁸ Treasury efforts to reduce vulnerabilities include providing alternative lines of communication for market participants. The department has also offered to provide secret physical security measures to key financial institutions requesting them.³⁹

A more concrete outline of Treasury's approach to the problems is its four-pronged overall approach to promoting continuity in the financial system and preventing interruption in case of a catastrophe. The focus first is on people. The second critical element is maintaining a high level of confidence in the functioning of the financial system. The third element is making sure that markets remain open — or, if they do close, reopen as quickly as possible. The final element is that resilience requires diversification if the primary place of business is nonfunctional.⁴⁰

In a specific cooperative modality, the Treasury has created a Protective Response Planning Program. This program brings together federal and local government officials, members of law enforcement and individuals from important

³⁶ Government officials describe initiatives in: U.S. Department of the Treasury. *Briefing Book on the Financial and Banking Information Infrastructure Committee and U.S. Department of the Treasury Critical Infrastructure Protection and Homeland Security Initiatives*, Nov. 14, 2002, at web site [<http://www.fbiic.gov>].

³⁷ "Treasury Introduces Upgrades Designed to Help Safeguard Financial Service System," *BNA's Banking Report*, Dec. 8, 2003, p. 836.

³⁸ Treasury Department Press Release, May 14, 2002, at web site [<http://www.treas.gov/press/releases/po3100.htm?IMAGE.X=35&IMAGE.Y=10>].

³⁹ Ben White, "Terrorism and the Markets: Officials Cite Improved Protections but Lingering Vulnerabilities," *Washington Post*, March 19, 2003, p. E3.

⁴⁰ Kip Betz, "Treasury Official Sees Progress in Crisis Preparedness Efforts," *Daily Report for Executives*, March 21, 2003, p.18.

financial institutions to develop and coordinate emergency responses to major disruptions at these specific institutions.⁴¹

OFHEO. Disaster recovery and back-up protocols mentioned in the Interagency Paper are seemingly also required by OFHEO—an independent office within the Department of Housing and Urban Development—in its safety and soundness examinations of the troubled government-sponsored housing finance enterprises it oversees. The latter, the Federal Home Loan Mortgage Corporation and Federal National Mortgage Association, are developing resilience internally as well.⁴²

Private Sector

FS-ISAC and Payments Networks. Y2K and other threats to financial companies had been feared for years. Many businesses sought to defend their operations in advance through hardware and software tests and upgrades. For example, they created the Financial Services Information Sharing and Analysis Center (FS-ISAC) in 1999. The nation's largest banking, securities, insurance, and investment firms participate in FS-ISAC, maintaining a database of security threats and system vulnerabilities, which they tie in with Treasury's bodies noted above.⁴³ Participants privately run FS-ISAC, like ISACs of all sectors. It is credited with safeguarding more than 1,300 financial institutions worldwide from any damage threatened by a computer virus targeted at them known as "Bugbear.B."⁴⁴ The Treasury Department has awarded a \$2 million contract to it to upgrade financial institution security and to increase its membership beyond the 50-plus largest critical firms.⁴⁵ Prominent funds transfer networks have strengthened their continuity plans both coordinatively with, and independently of, FS-ISAC.⁴⁶

Securities Industry. The Securities Industry Association (SIA) has released best practices guidelines for its members' recovery from disasters. SIA is also working with utility providers in New York to improve physical recovery measures. The New York Stock Exchange has developed back-up and redundancy facilities, although events did not damage its own facilities in the terror attacks. This exchange and the over-the-counter NASDAQ have agreed to trade each other's stocks if either were to become incapacitated. The National Association of Securities Dealers may

⁴¹ Department of the Treasury Press Release, Jan. 8, 2004, at web site [<http://www.treas.gov/press/releases/js1091.htm>].

⁴² Communication from Peter Brereton of OFHEO to William Jackson, April 3, 2003.

⁴³ "About FS-ISAC," at [<http://www.fsisac.com/aboutus.cfm>], visited April 15, 2003.

⁴⁴ David Hillis, "Industry Dodged Bugbear.B Virus," *American Banker Online*, June 11, 2003.

⁴⁵ U.S. Treasury Department Press Release, Dec. 9, 2003, on web site [<http://www.treas.gov/press/releases/js1047.htm>].

⁴⁶ David Breitkopf, "How Three Payment Networks are Remaking Contingency Plans," *American Banker Online*, Feb. 21, 2003; and, "Remarks by Vice Chairman Roger W. Ferguson, Jr. at Geneva, Switzerland, October 3, 2002," at web site [<http://www.federalreserve.gov/boarddocs/speeches/2002/20021003/default.htm>].

require business continuity plans of a similar nature. Measures that have been revealed include most securities firms having created backup sites far from New York, as the Interagency Paper suggested, and wiring a network linking broker/dealers to the New York and American Stock Exchanges through Consolidated Edison's underground pipes.⁴⁷

Banking Industry. As was noted above, extensive regulatory and supervisory protocols apply to banks as businesses. The potential for targeted cyber-disruption exists even for single banking firms. In 2003, the "SQL Slammer" worm shut down Bank of America Corp.'s Automated Teller Machines. Two large U.S. banks shut down their Machines after discovering that the "Welchia/Nochi" worm had attacked them.⁴⁸ Organizations such as "BITS," the technology arm of the Financial Services Roundtable trade group, focus on industry defenses. BITS estimates that bankers collectively spend more than \$1 billion on technology to mitigate cyber-threats annually. Daily patches are becoming industry practice.⁴⁹ Bankers may also purchase some insurance against liability for loss of customer confidential information through hacking, transmittal of a virus to customers from bank web sites, and denial of access when customers are unable to access information online because bank servers are down.⁵⁰

FSSCC. Organizations representing most significant financial entities have joined the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security.⁵¹ Its members, some of whom have self-regulatory oversight of their groups, cover most of America's finance, are the:

- American Bankers Association
- America's Community Bankers
- American Council of Life Insurers
- American Society for Industrial Security
- American Stock Exchange
- Bank Administration Institute
- BITS and Financial Services Roundtable
- Consumer Bankers Association
- Credit Union National Association
- Fannie Mae
- Financial Services Information Sharing and Analysis Center —
- Futures Industry Association
- Independent Community Bankers of America

⁴⁷ Greg Ip, "After Sept. 11, the U.S. Learned About Its Economic Resilience," *Wall Street Journal*, March 16, 2004, p. A15.

⁴⁸ David Breitkopf, "Worms, Crawling Through Windows, Menace ATMs," *American Banker Online*, Dec. 10, 2003

⁴⁹ Chris Constanzo, "Collaborating to Put Dent into \$1B Security Problem," *The American Banker Online*, Feb. 11, 2004.

⁵⁰ Lee Ann Gjertsen, "St. Paul Web-Risk Policy Offers Small-Bank Shield," *Ibid.*, November 07, 2003.

⁵¹ "Information," at web site [<http://www.fsscc.org/index.asp?template=info>].

- Investment Company Institute
- Managed Funds Association
- NASDAQ Stock Market, Inc.
- National Association of Federal Credit Unions
- National Automated Clearinghouse Association
- The (New York) Clearing House
- Securities Industry Association
- Securities Industry Automation Corporation
- The Bond Market Association
- The Options Clearing Corporation
- VISA USA Inc.

This body coordinates regularly and voluntarily with FBIIC.

Conclusion: Convergence of Private and Public Practices for Financial Recovery and Continuity

Many practices in the Interagency Paper came from financial firms' experiences and may thus be considered both public and private-sector ideas. Should the threat level increase, government expects critical private financial institutions to have security forces, identity checks, and restricted access, and to work with state and local authorities.⁵² The Fed, a body with both public and private elements,⁵³ remains ready to be the lender of last resort to the financial system and its customers as well. Recovery in the blackout of 2003, for example, was facilitated by the Fed, institutions activating internal contingency plans, as well as a paging and alert system set up after 9/11 by the Financial Services Roundtable (a group of major financial providers) and its technology arm BITS.⁵⁴

List of Major Acronyms

CFTC	Commodity Futures Trading Commission
DHS	Department of Homeland Security
FBIIC	Financial and Banking Information Infrastructure Committee
FDIC	Federal Deposit Insurance Corporation
Fed	Federal Reserve System

⁵² "Treasury Statement on Measures to Protect the Financial Markets during Hostilities."

⁵³ The Fed consists of a Board of Governors appointed by the President with the consent of the Senate, and 12 regional Federal Reserve Banks that issue voting stock in themselves to their owners, the "member commercial banks."

⁵⁴ Blackwell, "Backup Site Questions."

FS-ISAC	Financial Services Information Sharing and Analysis Center
FSSCC	Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security
GAO	General Accounting Office
NIAC	National Infrastructure Advisory Council
OCC	Office of the Comptroller of the Currency
OFHEO	Office of Housing Enterprise Oversight
SEC	Securities and Exchange Commission
TRIA	Terrorism Risk Insurance Act of 2002.