Order Code RL31873

CRS Report for Congress

Banking and Financial Infrastructure Continuity

Updated January 31, 2008

N. Eric Weiss
Analyst in Financial Economics
Government and Finance Division

Prepared for Members and
Committees of Congress

Banking and Financial Infrastructure Continuity

Summary

The Treasury Department and other agencies have long had the responsibility to ensure that the financial sectors of the economy are able to continue operations after physical and economic disruptions. This report outlines the financial sector's recovery plans for two kinds of disasters: the inability to conduct transactions and the large losses of asset value. The basic function of the payment system is carried out by banks, and monetary policy affects them immediately. Because brokers, exchanges, secondary market facilities, and insurance companies carry out crucial financial functions, their regulators and trade associations are involved in continuity of operations planning.

Regulators of financial entities have developed guidelines for regulatees to follow to cushion physical and economic shocks. There are procedures to protect business information technology, physical security, and for the continuity of markets critical for the nation's transactions. Government and private sector initiatives seek cost-effective ways to strengthen the resiliency of the financial system's computers against cyber attacks. Many of these arrangements protecting financial institutions against attacks are also part of the national effort to prevent terrorist financing from within the financial system. (See CRS Report RL33020, *Terrorist Financing: U.S. Agency Efforts and Inter-Agency Coordination*, by Martin A. Weiss, coordinator.) Defense of financial businesses' information systems is but one deterrence to national threats.

Following September 11, 2001, the nation became concerned with physical security. The anthrax attack in October 2001 heightened worries about biological terrorism. In 2004, the possibility of an avian flu pandemic concentrated continuity concerns on natural occurring challenges to the smooth functioning of the nation's financial system. Congress, regulators, and executive branch agencies have responded to each of these threats. This report[1] will be updated as events warrant.

[1] This report depends greatly on previous versions that were written and updated by William D. Jackson, who has retired from the Congressional Research Service.

Contents

Banking and Financial Infrastructure Continuity

Banking and Financial Institutions Form a Critical Infrastructure

Financial institutions, including banks, other depositories, securities dealers, insurers, and investment companies are part of the nation's critical infrastructure required for the nation's minimum economic operations.[2] Financial institutions accept funds from various sources and make them available as loans or investments to those who need them. America has vulnerabilities because its financial records are on computers and paper.

Financial institutions face two categories of emergencies that could impair their functioning. The first is directly financial: a sudden drop in the value of financial assets, whether originating domestically or elsewhere in the world, that could cause a national or even global financial crisis. The second is operational: the failure of the support structures that underlie the financial system. Either could disrupt the nation's ability to supply goods. They could reduce the pace of economic activity, or at an extreme, cause an actual contraction of economic activity.

Collapse of one prominent entity could evoke a contagion effect, in which sound financial institutions become viewed as weak and panicked customers withdraw funds from sound entities, causing them to fail. Regulators generally address financial problems through deposit insurance and other sources of liquidity (such as emergency loans) for distressed institutions, safety and soundness regulation, and direct intervention. They address operational risks through corrective actions (as with the Y2K problem), redundancy, regulation, auditing, and other physical security. Under the worst case scenarios, the Federal Reserve (Fed) can limit economic damage by supplying liquidity to the financial system and employing monetary policy to expand domestic demand (as it did following the 2001 terrorist attacks). In the Terrorism Risk Insurance Act of 2002 (TRIA), Congress expanded the Fed's ability

---

[2] CRS Report RL32631, *Critical Infrastructure and Key Assets: Definition and Identification*, by John Moteff and Paul Parfomak. Congress specified financial services as critical physical and information infrastructure in P.L. 107-56, Section 1016, Oct. 26, 2001. Banking and finance are critical infrastructure similar to telecommunications, water, etc. in *The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets*, at [http://www.whitehouse.gov/pcipb/physical.html]; *The National Strategy to Secure Cyberspace*, at [http://www.whitehouse.gov/pcipb]; "Homeland Security Presidential Directive/HSPD-7," at [http://www.whitehouse.gov/news/releases/2003/12/print/20031217-5.html]; and are expected to be clearly identified in a future written National Infrastructure Protection Plan (see *Federal Register*, vol. 7, no. 212, Nov. 3, 2005, p. 66840).

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 as it did in the cases of Chrysler, the Farm Credit System, and New York City to prevent them from defaulting, potentially causing failure in major parts of the financial system and the economy.

The Role of DHS

The Department of Homeland Security (DHS) is the government agency responsible for communications security oversight.[4] Financial institutions and their regulators operate in a different environment from nonfinancial ones. Financial intermediaries' most valuable assets are frequently business records that exist either as intangible computer records or as fragile paper documents. The financial sector rarely owns the external communications systems on which they depend. This lack of ownership limits the sector's ability to protect directly their vital communications. Protecting financial and banking computer hardware and software may require outside support.

DHS works with Treasury Department bodies concerned with financial security. Treasury assigns an expert in financial services matters on a rotating basis to DHS.[5] Following its move into DHS, the Secret Service, in cooperation with the Carnegie Mellon Software Institute, reviewed threats to information systems in critical financial infrastructures.[6] DHS has issued financial institution-specific alerts based on intelligence reports.[7]

Safety Net Measures in Place

This section offers a high level review of the powers of various financial regulators to intervene to prevent financial problems from spreading throughout the economy. It looks at both financial risks (those from a sudden decrease in value or a threat that financial intermediaries might not be able to honor their obligations to depositors) and physical risks (also known as operational and security risks).

---

[3] P.L. 109-144, which expires Dec. 31, 2007, extended P.L. 107-297. For a history and other information about TRIA, see CRS Report RS21979, *Terrorism Risk Insurance: An Overview*, and CRS Report RL33177, *Terrorism Risk Insurance Legislation: Issue Summary and Side-by-Side*, both by Baird Webel.

[4] "Administering the New Department of Homeland Security," at [http://www.congress.gov/erp/legissues/html/isdhs2.html].

[5] "Treasury Introduces Upgrades Designed To Help Safeguard Financial Service System," *BNA's Banking Report*, Dec. 8, 2003, p. 836.

[6] U.S. Secret Service, "Secret Service and CERT Coordination Center Release Comprehensive Report Analyzing Insider Threats to Banking and Finance Sector," press release, at [http://www.secretservice.gov/press/pub1804.pdf].

[7] Derrick Cain, "Nation's Banks Conduct 'Business as Usual' After Specific Threats to Certain Institutions," *BNA's Banking Report*, Aug. 9, 2004, p. 221.

Financial Risks

Financial regulation includes deposit insurance, safety and soundness oversight, and the Fed as lender of last resort and ultimate protector of the financial system. Many arrangements protect financial institutions and their customers from different kinds of risk.[8]

The Fed has long stood ready to provide liquidity in the form of emergency loans to the banking system. The Federal Deposit Insurance Corporation (FDIC) protects depositors against failure of a bank or savings association. This insurance helps to prevent depositor panics that could drain banks of their funds, and in turn could lead to curtailed lending and calling in loans. Even a healthy depository institution, otherwise untouched by any cause of failure, could not long withstand a depositor panic.

The FDIC brings order to the process of resolving insolvent banks. 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 for rescue operations. Credit unions have similar arrangements with their Central Liquidity Facility and Share Insurance Fund. The Pension Benefit Guaranty Corporation (PBGC) guarantees pension funds with defined benefits.

The securities industry lacks a pool of emergency liquidity, but the Fed may, if it chooses, lend directly to securities firms. The federal government protects individual securities accounts against operational losses — although not collapses of market value — through the Securities Investor Protection Corporation.[9] Each state has a guaranty fund to make good the obligations of an insolvent state-regulated insurance companies, although there is no national liquidity pool. TRIA provides a federal backstop for insurers willing to provide terrorism insurance. This law is designed to assure that such insurance remains available by protecting providers against catastrophic losses in case of terrorist attacks.

Other agencies bolster the national financial safety net maintaining confidence in many other ways. Not all of these entities provide liquidity or rescue in the case of financial failure. For many years, the securities industry and issuers have had overseers and programs designed to prevent a collapse in confidence originating within the system. The Securities and Exchange Commission (SEC) has sought transparency (disclosure) in the financial practices of businesses whose securities are traded in public markets. The Sarbanes-Oxley Act of 2002 sought to restore investor confidence by strengthening the regulation of independent auditors and by increasing the accountability of corporate executives and directors.[10] The Federal Housing Finance Board and the Office of Federal Housing Enterprise Oversight regulate

---

[8] CRS Report RS21987, *When Financial Businesses Fail: Protection for Account Holders*, by William D. Jackson.

[9] CRS Report RS21741, *Securities Investor Protection Corporation*, by Gary Shorter.

[10] P.L. 107-204, July 30, 2002.

safety and transparency of important non-depository housing finance institutions.[11] The Commodity Futures Trading Commission (CFTC) oversees organized markets on futures and similar contracts through self-regulatory organizations.

Every state regulates its state-chartered banks, credit unions, thrift institutions, and companies engaged in securities and futures operations. Although state-chartered depository institutions are subject to federal regulation, the states are the primary regulators for 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. State regulatory bodies for their respective industries are linked through the 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. With TRIA, Congress strengthened the Fed's authority to lend to businesses directly in "unusual or exigent circumstances."[12]

Operational and Security Risks

Safety and soundness regulators issue guidelines and specific regulations for redundancy and security in physical and financial systems. They have long required banking institutions to consider operating (security) risks in contingency planning, and now include risk of catastrophic disruptions such as occurred on September 11, 2001. The securities industry is refining its procedures along similar lines. Insurance and other non-depository, non-securities financial businesses have not revealed their continuity plans. Although vital, they are not considered as critical. Few would regard the inability to process car loans, for example, as serious a problem as the inability to process checks and securities.

Safety and Continuity in Recent Experience

This section reviews the major financial disruptions since the stock market crash of 1987 and how the government responded to reduce the chance that the disruption could spread and cause severe finance and economic problems.

Last Decades of 1900s. Sudden drops in the value of financial assets that affected the U.S. financial system late in the 20th century include the 1987 stock market crash, the savings and loan and banking collapses of 1989-1991, and the 1997-1998 Asian and Russian financial crises. The Fed and other financial regulators

---

[11] CRS Report RL32815, *Federal Home Loan Bank System: Policy Issues*, by Barbara Miles.

[12] CRS Report RS21986, *Federal Reserve: Lender of Last Resort Functions*, by Marc Labonte.

responded by providing liquidity to the banking system, and so to the economy. Following the 1987 stock market crash, several regulatory agencies and the President's Working Group on Financial Markets issued many recommendations that became practice.[13] That group issued another study, with recommendations, in the late 1990s when international disturbances threatened the United States through the near collapse of the Long-Term Capital Management hedge fund. It examined problems that financial derivatives posed to the economy in 1999. Congress passed reforms of federal deposit insurance and banking regulators' authorities over practices threatening depository institutions in 1989 and 1991.[14] 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.

2000 — Y2K. The operational safety net created to defend against computer problems feared for the Year 2000 (Y2K) worked. The widely anticipated Y2K bug was a software programming problem that could have caused failures in the infrastructure upon which the system relies. Public and private groups worked hard to prevent the widely feared collapse of financial capabilities on January 1, 2000. Y2K came and went without serious incident and the systematic backups and safeguards provided against it proved invaluable the following year.

2001 — September 11. With the September 11, 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 liquidity to prevent panic. It injected more than $100 billion into the banking system. It arranged international facilities to keep the global financial system operating. The Fed and central banks around the world cut interest rates and lent money to banks to ease pressures on borrowers.

The SEC issued emergency rules encouraging buying when the stock markets reopened. Trading recommenced rapidly, as the U.S. Treasury security market reopened on September 13, and the equities market was in full operation on September 17. Physical infrastructure recovery required 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 records and communications systems by institutions outside the attack area allowed quick resumption of near-normal operations. 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 stopped writing insurance covering terrorist-related claims. This led TRIA to encourage insurers to write terrorism risk insurance. Nevertheless, some high-profile commercial properties lack terrorism insurance because of the high cost of such

---

[13] This group consists of the Treasury, Fed, SEC, and CFTC.

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

protection in spite of TRIA. The government also provides insurance to domestic airlines under the Air Transportation Safety and System Stabilization Act.[15]

2003 — Blackout. Emergency response measures noted above helped reduce the financial market damages from the August 14, 2003 power blackout in the northeastern United States and Canada. Treasury 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 majority of stock, options, commodities, futures, and bonds markets soon returned to normal operation. Banks closed affected offices in New York and Detroit; elsewhere, financial systems operated normally. The Fed's payments and emergency lending systems operated well. Banks borrowed and repaid $785 million from the Fed after the blackout, the most since the week after September 11. Applications for new mortgages fell temporarily because of the blackout. Contrary to initial fears, terrorists had not caused the blackout, and the blackout did not severely stress the nation's financial economy.[16]

2004 — Hurricanes. Several financial institutions in the southern and eastern United States had to suspend operations in areas affected by hurricanes and tropical storms in 2004. Federal and state regulators issued orders allowing banks in areas affected by Hurricanes Bonnie, Charley, Frances, Ivan, and Jeanne to suspend operations. Despite large payouts for storm-related damage to many sectors, the insurance sector rebounded.

2004 — Orange Alert. Financial institutions received warnings of an elevated threat level in August 2004, raising concerns about the possibility of another September 11 event. Although no such threats materialized, public and private preparations were made appropriately.

2005 — Hurricanes. Almost all of the financial sector's protections put in place in recent years had to be activated regionally due to the hurricanes of 2005. Hurricane Katrina disrupted both power and communications in parts of Mississippi, Alabama, and Louisiana. Cash could not be withdrawn, checks could not be cashed, and debit and credit card networks (including ATMs) were down. In addition, facilities of a number of financial institutions were destroyed by wind or made inaccessible by water. Continuity of operations procedures, which are required of all but the smallest depository institutions, include maintaining critical personnel and data storage (with daily backups) at sites located at least 20 miles from a bank's headquarters. In almost every case, data backups worked despite loss of electricity. Joint guidance provided by the four federal bank regulators, and independently by the National Credit Union Administration, advised a temporary easing of regulations,

---

[15] P.L. 107-42, Sept. 22, 2001.

[16] "Measures Prompted by Sept. 11 Helped Banks Weather Electrical Outage, Snow Says," *BNA's Banking Report*, Aug. 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," *American Banker Online*, Aug. 18, 2003. (Hereafter cited as Blackwell, *Backup Site Questions*.)

facilitating recovery. (See CRS Report RS22263, *Katrina's Wake: Restoring Financial Services*, by Barbara L. Miles.)

Insurance claims did not threaten the industry. Insured losses from Hurricane Katrina are estimated at $40.6 billion.[17] Nevertheless, the U.S. property-casualty insurance industry's net income after taxes rose by more than 4% during that time.[18] Increasing premiums seem inevitable in affected areas, thereby strengthening industry surpluses and viability.

Financial Business Continuity Initiatives

The payments system continued to function after the attack on New York's financial activity. Providers realize that coordination between their primary site and one or more backup sites needs to be improved.

The banking sector now functions normally. Despite initial concerns over safety, deposits inflows continued and profits were high even while borrowing slowed. Bond trading levels have recovered to their previous volume despite devastation of Cantor Fitzgerald, the company responsible for most of the market for government bonds. The stock markets recovered. With the federal backstop for insurers, coverage of acts of terrorism is available, although with higher premiums.

Regulatory Initiatives

This section examines the changes that financial regulators have made to improve the resilience of the nation's financial system since September 11, 2001, and plans for future changes.

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 Office of the Comptroller of the Currency (OCC), and the SEC issued a white paper called *Structural Change in the Settlement of Government Securities*. That paper expressed concerns about operational, financial, and structural vulnerabilities from having only two clearing banks. In response, the Fed initiated a number of measures including a backup dormant clearing and settlement bank, ready to act

---

[17] Insurance Information Institute, "Nearly 95 Percent of Homeowners Claims from Hurricane Katrina Settled and Tens of Billions of Dollars Paid to Affected Communities in Louisiana and Mississippi, Insurance Information Institute Reports," Aug. 22, 2006, at [http://www.iii.org/media/updates/press.760032/].

[18] "In Brief: Despite Storms, P/C Profits Grew 4.4%," *American Banker Online*, Dec. 29, 2005.

should the two banks clearing government securities transactions be unable to do so.[19]

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 firms access to priority emergency communications.[20] These programs, which the National Communications System administers, help financial markets overcome substantial operational disruptions. They are (1) Telecommunications Service Priority for circuits used in large-value interbank funds transfer, securities pricing and transfer, and payment-related services, (2) Government Emergency Telecommunications Service (GETS) for priority calls over terrestrial public switched networks, and (3) Wireless Priority Service of cellular calls during severe network congestion. The GETS program is now available to all financial institutions.[21]

Sound Practices Paper. 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*.[22] The *Sound Practices* paper covers the largest wholesale financial sector businesses. It does not address retail or trading operations, nor the insurance sector. The regulators directed financial institutions involved in financial clearing and settlement activities to adopt the paper's guidance. This provides 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.[23]

The *Sound Practices* paper analyzes the risks of 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 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 lists four 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,

---

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

[20] At [http://www.occ.treas.gov/ftp/bulletin/2003-13.txt].

[21] R. Christian Bruce, "GETS Cards Urged for Financial Institutions To Ensure Smooth Communications in Crises," *BNA's Banking Report*, Dec. 6, 2004, p. 859.

[22] *Federal Register*, vol. 68, no. 70, Apr. 11, 2003, pp. 17809-17814.

[23] At [http://www.occ.treas.gov/ftp/bulletin/2003-14.txt].

- maintain sufficient geographic dispersion of resources to meet recovery and resumption activities, and
- routine use or test recovery and resumption arrangements.

This paper requires robust backup facilities for clearance and settlement activities, resumption of normal business within two hours, regular testing of backup facilities, and backup personnel. They did not recommend moving primary offices of financial and securities firms, contrary to some expectations. In April 2006, the three regulatory agencies reported that the recommendations were substantially in place.[24]

Federal Financial Institutions Examination Council. The four bank and one credit union regulatory agencies constitute the Federal Financial Institutions Examination Council (FFIEC). This council's information technology subcommittee coordinates agency policies on technological and related risks, including security procedures and financial business continuity.[25] Following the damage of Hurricane Katrina, banking agencies formed a working group to coordinate emergency responses on both state and national levels to "provide institutions with clear, timely, and consistent information on areas of concern."[26]

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 a controversial requirement for covered firms to carry more capital for operational risk.[27] Operational risk refers to the risk of loss resulting from flawed internal processes, people and systems, and external events. Hearings by two subcommittees of the House Financial Services Committee in 2003 explored some of its implications, which many bankers feel are burdensome.[28] A 109th Congress measure, United States Financial Policy Committee for Fair Capital Standards Act, H.R. 1226, would address Basel II, including its

---

[24] Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency, and Securities and Exchange Commission, *Joint Report on Efforts of the Private Sector to Implement the Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*, April 2006, at [https://www.fsscc.org/reports/2006/Sound_Practices_Status_Report.pdf].

[25] Rob Blackwell, "Regulators Put Examiner Update Online," *American Banker Online*, Jan. 30, 2003.

[26] See [http://www.ffiec.gov/press/pr091905.htm].

[27] See CRS Report RL33278, *The Basel Accords: The Implementation of II and the Modification of I*, by Walter W. Eubanks.

[28] U.S. Congress, House Committee on Financial Services, Subcommittee on Domestic and International Monetary Policy, Trade and Technology, *The New Basel Accord — Sound Regulation or Crushing Complexity?*, hearing on H.Hrg. 108-5, 108th Cong., 1st sess., Feb. 27, 2003 (Washington: GPO, 2003), at [http://financialservices.house.gov/hearings.asp?formmode=detail&hearing=182]; and House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit, *The New Basel Accord — in Search of a Unified U.S. Position*, hearing on H.Hrg. 108-40, 108th Cong., 1st sess., June 19, 2003, (Washington: GPO, 2003), at [http://financialservices.house.gov/hearings.asp?formmode=detail&hearing=236].

operational risk component. A similar bill in the 108th Congress (H.R. 2043) was marked up in subcommittee.

Executive Branch Initiatives

This section reports on the actions of executive branch agencies to improve their ability to function financially following a catastrophic event. Public-private groups are also discussed.

Government's Own Financing. The E-Government Act of 2002 requires financial offices within the federal government to develop, document, and carry out agency-wide information security programs.[29] Treasury and other agencies have taken steps to protect the government's critical financial functions, including borrowing, making payments (including Social Security), and collecting taxes. Should the threat level rise, agencies will work with state and local governments to increase physical and cyber security measures, disperse individuals critical to operations, and activate backup facilities.[30]

Presidential. President Bush has appointed executives of the banking and securities industries to the National Infrastructure Advisory Council (NIAC). The panel advises the White House on cyber security and information security of critical economic infrastructure, including financial ones. Members of NIAC represent major sectors of the economy: banking and finance, transportation, energy, information technology, and manufacturing. It includes representatives from academia, state and local government, and law enforcement. NIAC works closely with the President's National Security and Telecommunications Advisory Committee.[31]

NIAC meets periodically to

- 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,
- encourage private industry to perform periodic risk assessments of critical information and telecommunications systems,
- 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,

---

[29] P.L. 107-347, Dec. 17, 2002.

[30] Department of the Treasury, "Treasury Statement on Measures to Protect the Financial Markets during Hostilities with Iraq," press release, Mar. 17, 2003, at [http://www.treas.gov/press/releases/ js114.htm].

[31] Department of the Treasury, "Appointments to National Infrastructure Advisory Committee," press release, Sept. 18, 2002, at [http://www.whitehouse.gov/news/releases/2002/09/20020918-12.html].

- 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
- advise lead agencies with critical infrastructure responsibilities, sector coordinators, DHS, and ISACs, including for the banking and finance sector.[32]

In 2003, Presidential Homeland Security Directive 7 assigned sectoral protection responsibility to departments and agencies based on their expertise in infrastructures.[33] Treasury is the sector-specific agency for the banking and finance sector and operates through numerous channels noted below.[34]

Financial and Banking Information Infrastructure Committee. Treasury's Office of Critical Infrastructure Protection, formed after September 11, staffs the Financial and Banking Information Infrastructure Committee (FBIIC). Its chair is Treasury's Assistant Secretary for Financial Institutions.[35] Its mission is to coordinate federal and state efforts to improve the reliability and security of the financial system.[36] A public sector group, FBIIC was created by executive order in 2001 and includes representatives of the following:

- Commodities Futures Trading Commission
- Conference of State Bank Supervisors
- Department of the Treasury
- Farm Credit Administration
- Federal Deposit Insurance Corporation
- Federal Housing Finance Board
- Federal Reserve Bank of New York
- Federal Reserve Board
- National Association of Insurance Commissioners
- National Association of State Credit Union Supervisors
- National Credit Union Administration
- North American Securities Administrators Association
- Office of the Comptroller of the Currency

---

[32] Department of the Treasury, "Executive Order Amendment of Executive Orders, and Other Actions, in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security," press release, Feb. 8, 2003, at [http://www.whitehouse.gov/news/releases/2003/02/20030228-8.html].

[33] "Homeland Security Presidential Directive/HSPD-7," at [http://www.whitehouse.gov/news/releases/2003/12/print/20031217-5.html].

[34] Statement by Scott D. Parsons, "Financial Market Preparedness for Wide-Scale Disasters or Disruptions: A Treasury Perspective," before the Subcommittee on Government Management, Finance, and Accountability of the House Committee on Government Reform, Sept. 26, 2005, at [http://www.treas.gov/press/releases/js2950.htm].

[35] It was the Office of Homeland Security's Financial Markets Work Group.

[36] Financial and Banking Information Infrastructure Committee (FBIIC), at [http://www.fbiic.gov].

- Office of Federal Housing Enterprise Oversight
- Office of Thrift Supervision
- Securities and Exchange Commission
- Securities Investor Protection Corporation

FBIIC conducts vulnerability assessments of the retail payment system, government-sponsored enterprises (such as Fannie Mae, Freddie Mac, and the Federal Home Loan Banks), and the insurance industry — none directly addressed in the *Structural Change* report — and other improvements to financial resiliency.[37] Treasury has procedures for secure communications between federal and state regulators to share information about an event affecting their regulated financial institutions.[38] FBIIC has analyzed how to counter "phishing" attacks against financial institutions, and how financial institutions recovered from Hurricane Isabel.[39] It met frequently during the events surrounding Katrina.[40]

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.[41] Treasury efforts to reduce vulnerabilities include providing alternative lines of communication for market participants. The department provides secret physical security measures to key financial institutions requesting them.[42]

Treasury has a 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

---

[37] 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 [http://www.fbiic.gov].

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

[39] Published results are found at [http://www.treas.gov/offices/domestic-finance/financial-institution/cip].

[40] Statement by Scott D. Parsons, "Financial Market Preparedness for Wide-Scale Disasters or Disruptions: A Treasury Perspective," before the Subcommittee on Government Management, Finance, and Accountability of the House Committee on Government Reform, Sept. 26, 2005, at [http://www.treas.gov/press/releases/js2950.htm].

[41] Department of the Treasury, "Treasury Names Private Sector Coordinator for Critical Infrastructure Protection Partnership Effort," press release, May 14, 2002, at [http://www.treas.gov/press/releases/po3100.htm?IMAGE.X=35\&IMAGE.Y=10].

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

element is that resilience requires diversification if the primary place of business is nonfunctional.[43]

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 financial institutions to develop and coordinate emergency responses to major disruptions regionally.[44] One such cooperative network, ChicagoFIRST, is a model for similar activities around the nation and is described below.

Department of Justice. Independent of other efforts, the Department of Justice has developed a set of *Suggested Best Practices on Computer and Internet Security for Financial Institutions*.[45] The document informs financial firms of national resources available to them as well.

Private Sector Initiatives

This section summarizes the actions of businesses to improve their ability to survive major economic and financial disruptions. It also reports on public-private collaboration.

FS-ISAC and Payments Networks. Y2K and other threats to financial companies had been feared for years. Many businesses defended their operations through hardware and software tests and upgrades. For example, they created the Financial Services-Information Sharing and Analysis Center (FS-ISAC) in 1999. Nearly 1,000 banking, securities, insurance, and investment firms participate in FS-ISAC, maintaining a database of security threats and system vulnerabilities, which they tie in with the previously noted Treasury bodies.[46] Participants privately run FS-ISAC, like ISACs of 14 sectors. Observers have credited it with safeguarding more than 1,300 financial institutions worldwide from any damage threatened by a computer virus targeted at them known as Bugbear.B.[47] Treasury awarded FS-ISAC a $2 million contract to upgrade financial institution security and to increase its membership.[48] Prominent funds transfer networks and securities exchanges have

---

[43] Kip Betz, "Treasury Official Sees Progress in Crisis Preparedness Efforts," *Daily Report for Executives*, Mar. 21, 2003, p.18.

[44] Department of the Treasury, "Remarks of Michael A. Dawson, Deputy Assistant Secretary for Critical Infrastructure Protection and Compliance Policy," *Protecting the Financial Sector from Terrorism and Other Threats*, press release, Jan. 8, 2004, at [http://www.treas.gov/press/releases/js1091.htm].

[45] At [http://www.fbiic.gov/reports/Best_Practices_Network_Security.doc].

[46] "About FS-ISAC," at [http://www.fsisac.com/aboutus.cfm].

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

[48] U.S. Treasury Department "Remarks of Acting Under Secretary of the Treasury for Domestic Finance, Brian Roseboro on the Next Generation Financial Services Information Sharing and Analysis Center," press release, Dec. 9, 2003, at

(continued...)

strengthened their continuity plans both independently and in conjunction with FS-ISAC.[49] Through the private sector Partnership for Critical Infrastructure Security, FS-ISAC meets quarterly with sector coordinators for each of the critical national infrastructure sectors. It continues to function actively in public-private partnership and outreach modes, including making defenses available against phishing criminal cyber activity seeking to steal financial data.[50]

Securities Industry. The Securities Industry Association (SIA) has released disaster recovery best practices for its members. SIA is working with utility companies in New York to improve physical recovery measures. Although the September 11 terror attacks did not damage its facilities, the New York Stock Exchange (NYSE) has developed backup and redundancy facilities. The NYSE and NASDAQ have agreed to trade each other's stocks if either were to become incapacitated. The NYSE and National Association of Securities Dealers (NASD) have mandated business continuity plans. Measures revealed by the industry require that most securities firms have backup sites far from New York, as the *Sound Practices* paper suggested, and a wired network to the stock exchange through Consolidated Edison's underground pipes.[51] In cooperation with the FBIIC, SIA conducted a wide-ranging test of emergency procedures in October 2005 that was viewed it as successful.

Banking Industry. Extensive regulatory and supervisory procedures apply to banks as businesses. The potential for targeted cyber disruption exists even for single banking firms. Organizations such as the Banking Industry Technology Secretariat (BITS), the technology arm of the Financial Services Roundtable trade group, focus on industry defenses. It is a nonprofit consortium of the largest 100 financial institutions in the country dealing with strategic approaches to crisis management and payments systems. BITS estimates that bankers collectively spend more than $1 billion annually on cyber security. Daily patches are becoming an industry practice.[52] Bankers may purchase insurance against liability for loss of customer confidential information through hacking, transmittal of a virus to customers from bank website, and denial of access when customers are unable to get to information because bank servers are down.[53]

---

[48] (...continued)
[http://www.treas.gov/press/releases/js1047.htm].

[49] 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, Oct. 3, 2002," at [http://www.federalreserve.gov/boarddocs/speeches/2002/20021003/default.htm].

[50] Financial Services Sector Coordinating Council, *Protecting the U.S. Critical Infrastructure: 2004 in Review* (New York: 2005), p. 5.

[51] "After Sept. 11, the U.S. Learned About Its Economic Resilience," *Wall Street Journal*, Mar. 16, 2004, p. A15.

[52] Chris Constanzo, "Collaborating to Put Dent into $1B Security Problem," *American Banker Online*, Feb. 11, 2004.

[53] Lee Ann Gjertsen, "St. Paul Web-Risk Policy Offers Small-Bank Shield," *American* (continued...)

Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security. Organizations representing financial entities have created the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security, called FSSCC for short. It is essentially a private-sector counterpart to FBIIC. Its members, some of whom have self-regulatory oversight of their groups, cover most of America's finance. Its mission is to identify opportunities for coordination, improve knowledge and information sharing, and improve public confidence in sectoral recovery from terrorist attacks and other illegal activities. Its members are

- American Bankers Association
- America's Community Bankers
- American Council of Life Insurers
- American Insurance Association
- American Society for Industrial Security International
- Bank Administration Institute
- Bond Market Association
- ChicagoFIRST
- Chicago Mercantile Exchange
- CLS Group (foreign exchange)
- (New York) Clearing House
- Consumer Bankers Association
- Credit Union National Association
- Depository Trust and Clearing Corporation
- Fannie Mae
- Financial Information Forum
- Financial Services Information Sharing and Analysis Center
- Financial Services Roundtable/BITS
- Financial Services Technology Consortium
- Futures Industry Association
- Independent Community Bankers of America
- Investment Company Institute
- Managed Funds Association
- NASDAQ Stock Market, Inc.
- National Association of Federal Credit Unions
- National Association of Securities Dealers
- National Automated Clearinghouse Association
- New York Board of Trade
- Options Clearing Corporation
- Securities Industry Association
- Securities Industry Automation Corporation
- VISA USA Inc.

FSSCC holds quarterly meetings with FBIIC.[54]

---

[53] (...continued)
Banker Online, Nov. 7, 2003.

[54] Financial Services Sector Coordinating Council, *Protecting the U.S. Critical* (continued...)

Another example of the multiplicity of connections to strengthen financial industry resiliency is ChicagoFIRST, a regional coalition augmenting nationwide information sharing and policy initiatives. Formed in 2003 when Chicago's financial institutions decided that after September 11 they were as vulnerable as those in New York, it includes many members of FSSCC listed above and Illinois governments. A limited liability company funded by its for-profit members, it has developed defensive capabilities that are recognized as a model for other regional arrangements to fortify specific areas.[55]

In the communications arena, FSSCC member organizations have developed contact procedures to coordinate industry members and governmental bodies during emergencies, and merged these connections into a common database.

Legislation and Oversight

This section reports on congressional action in response to disruption to the nation's economy.

Post-September 11 Legislation

Following the attacks of September 11, 2001, Congress created DHS by combining all or part of 22 different agencies.[56] DHS has responsibilities previously assigned to 22 agencies to protect communications, transportation, and computer networks. These networks are critical to the financial sector's ability to transform data into useful forms of information such as bank account balances, securities prices, orders to buy and sell financial assets, and payments on contractual obligations such as loans.

Congress passed TRIA to backstop terrorism insurance for property-casualty insurers and airlines. Other congressional measures, including tax relief for investors and financial integrity initiatives increased confidence in the securities markets by 2003. The House approved a bill to give the SEC additional authority in a national emergency, on February 26, 2003. The Emergency Securities Response Act, H.R. 657, would have allowed the SEC to extend emergency orders beyond the 10 business days currently allowed. It also would have expanded the agency's ability to grant exemptions from federal securities laws. Emergency powers could have extended for any period specified by the commission up to 90 calendar days. The House had approved a similar bill in 2001, which the Senate did not take up either.

---

[54] (...continued)
Infrastructure, p. 1-65.

[55] U.S. Department of the Treasury, *Improving Business Continuity in the Financial Services Sector: A Model for Starting Regional Coalitions* (Washington: 2004), 38 p.

[56] P.L.107-296

Intelligence Reform and Terrorism Prevention Act of 2004. Beyond anti-terrorist tactics and financing legislative recommendations, the September 11 Commission's findings led to major financial preparedness legislation. The resulting Intelligence Reform and Terrorism Prevention Act of 2004, P.L. 108-458, requires DHS to report on vulnerability and risk assessments and the government's plans to protect infrastructures, including financial institutions.

Treasury is required to report on "the effectiveness and efficiency of efforts to protect the critical infrastructure of the United States financial system ...." Treasury is to report on its efforts to encourage public-private partnerships to protect critical financial infrastructure. Treasury also has authority for government securities market disturbances parallel to the SEC's authority.

After consulting with Treasury, the Fed, and the Commodity Futures Trading Commission, the SEC is authorized to issue orders and take other emergency actions to address extraordinary private securities market disturbances.

The Fed, the OCC, and the SEC are to report on private sector financial business continuity plans, including more financial services entities than are under existing regulation. The agencies published their guidance in the *Sound Practices* noted above.

The law urges insurance and credit rating companies to consider businesses' compliance with private sector standards in assessing insurability and creditworthiness, to encourage private investment in disaster and emergency preparedness.

The law increases governmental and private emergency preparedness planning. It encourages financial businesses smaller than the largest wholesale transacting and clearing entities, the only firms now covered by the *Sound Practices* paper, to undertake emergency preparedness. The insurance and credit rating provision reflects concerns over lending and insuring in areas subject to flooding and the like, where planning against consequences of disasters is highly relevant.

Congressional Oversight

The Government Accountability Office (GAO) has reviewed threat mitigation in financial markets and reported its findings to Congress. One study recommended that Treasury coordinate with the financial industry to update the sector's National Strategy for Critical Infrastructure Assurance and to improve the process for monitoring its progress. GAO suggested that Treasury assess the need for grants, tax incentives, regulation, or other public policy tools.[57]

---

[57] U.S. Government Accountability Office, *Critical Infrastructure Protection: Efforts of the Financial Services Sector to Address Cyber Threats*, GAO-03-173, Jan. 30, 2003, at [http://www.gao.gov].

Another review found deficiencies in the Treasury-Federal Reserve Internet payments system known as pay.gov, which seem to have been fixed.[58]

Other recommendations from GAO studies include

- increasing information security controls at Treasury,[59]
- strengthening access controls to the Federal Reserve's system for Treasury bond auctions,[60] and
- creating an emergency backup system to replace the system for financing the government under which the Federal Reserve Bank of New York auctions bonds and bills for the Treasury.[61]

Congress examined some of the agency's findings in a hearing by the House Financial Services Subcommittee on Capital Markets, Insurance and Government-Sponsored Enterprises held February 12, 2003.[62] GAO found that the Fed, the OCC, and the SEC lacked a strategy for having their regulatees resume trading in securities following any 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 risk mitigation.

Developing Concerns: Pandemic Flu

In the past couple of years, the nation has become concerned about the possibility of a pandemic flu outbreak. Large scale illness, mass absenteeism, quarantines, and death could disrupt the nation's financial system. Proposals have been made to increase teleworking and alternative work locations to contain the spread of the flu. The Department of Health and Human Services is the lead agency

---

[58] U.S. Government Accountability Office, *Information Security: Computer Controls over Key Treasury Internet Payment System*, GAO-03-837, July 30, 2003, [http://www.gao.gov].

[59] U.S. Government Accountability Office, *Improvements Needed in Treasury's Security Management Program*, GAO-04-77, Nov. 2003, [http://www.gao.gov/new.items/d0477.pdf].

[60] U.S. Government Accountability Office, *Information Security: Federal Reserve Needs to Address Treasury Auction Systems*, GAO-06-659, Aug. 30, 2006, at [http://www.gao.gov/new.items/d06659.pdf].

[61] U.S. Government Accountability Office, *Debt Management: Backup Funding Options Would Enhance Treasury's Resilience to a Financial Market Disruption*, GAO-06-1007, Sept. 2006, at [http://www.gao.gov/new.items/d061007.pdf].

[62] U.S. Government Accountability, *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 Feb. 12, 2003, through GAO's website [http://www.gao.gov]. "Recovery and Renewal: Protecting the Capital Markets Against Terrorism," at [http://financialservices.house.gov/hearings.asp?formmode=detail&hearing=176].

for government planning. It has created a special website that includes a check list for business planning, at [http://www.pandemicflu.gov]. DHS has held regional meetings around the nation to encourage businesses and governments to plan for disruptions.

The same public and private groups that have worked to develop continuity of operations plans to recover after a terrorist attack have also worked together to plan for a pandemic. There is a consensus that although a pandemic would cause many of the same problems as a terrorist attack, it could be different. A pandemic could be worldwide, but have local concentrations requiring unprecedented coordination and communication between financial regulators, the private sector, public health officials, school officials, public transportation, mass transit, the communications sector and police.

The FSSCC has examined this problem from the perspective of banks and bank regulators, including compliance with the new proposed risk-based capital standards known as Basel II.[63] Their report emphasizes the need to minimize physical contact among employees, customers, and the supply chain, being able to operate with key staff incapacitated, and to have contingency plans if suppliers cannot deliver goods and services.

A joint flu preparedness exercise by FSSCC, Treasury, the Department of Homeland Security, and the Securities Industry and Financial Management Association simulate an influenza pandemic with absenteeism rates reaching 49%.[64] The goals of the October 2007 exercise were (1) to enhance industry understanding of system risks from flu; (2) to provide an opportunity to test plans for a flu pandemic; and (3) to study how a flu pandemic would affect the financial structure. Over 98% of the 2,550 participating organizations said it helped them in their continuity planning.

A GAO study found that many government agencies would have essential team members telecommute during a pandemic, but that very few had tested their plans.[65]

A flu pandemic is not just a concern of the United States. The International Monetary Fund has published a report that, in part, addresses the problems that could confront financial institutions.[66] These include continuity of operations, increased

---

[63] Patrick McConnell, *Banks and Avian Flu: Planning for a Possible Pandemic*, undated, at [https://www.fsscc.org/influenza/banks_and_avian_flu_planning.pdf].

[64] Financial Banking Information Infrastructure Committee and Financial Services Sector Coordinating Council, *FBIIC/FSSCC Pandemic Flu Exercise: Media Briefing*, October 24, 2007. Available at [http://www.treasury.gov/press/releases/reports/panfluhandout.pdf].

[65] Statement of David M. Walker, "Continuity of Operations: Agencies Could Improve Planning for Telework during Disruptions," before the House Committee on Government Reform, May 11, 2006, at [http://reform.house.gov/UploadedFiles/GAO%20-%20Walker%20Flu%202006%20Opener.pdf].

[66] International Monetary Fund, *The Global Economic and Financial Impact of an Avian Flu Pandemic and the Role of the IMF*, Feb.28, 2006 at
(continued...)

delinquency and default on loans due to illness at borrowers' business and business disruption. The IMF recommended that financial business plans for a contagious outbreak, including provisions in case key staff become ill and for working from multiple locations. Other suggestions included finding ways for staff to commute without mass transit.

Conclusion: Convergence of Public-Private Practices for Financial Continuity

The private and public sectors have worked together to document and build on the lessons learned from the terrorist attacks of September 11 and other disruptions. Regulators and special purpose groups have monitored the implementation of best practices to the common goal of minimizing future disruptions. This has been done by persuasion, regulation, rule, and law.

Although much of the original impetus was a terrorist attack, the new policies have worked well during natural disasters such as hurricanes and have been the basis for planning to mitigate the disruption of a flu pandemic.

---

[66] (...continued)
[http://www.imf.org/external/pubs/ft/afp/2006/eng/022806.pdf].

Appendix: Major Acronyms

BITS	Banking Industry Technology Secretariat
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
FS-ISAC	Financial Services-Information Sharing and Analysis Center
FSSCC	Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security
GAO	Government Accountability Office
NIAC	National Infrastructure Advisory Council
OCC	Office of the Comptroller of the Currency
PBGC	Pension Benefit Guaranty Corporation
SEC	Securities and Exchange Commission
TRIA	Terrorism Risk Insurance Act of 2002