Banking and Financial Infrastructure Continuity: Pandemic Flu, Terrorism, and Other Challenges

N. Eric Weiss
Specialist in Financial Economics

May 4, 2009

Congressional Research Service
7-5700
www.crs.gov
RL31873

CRS Report for Congress
Prepared for Members and Committees of Congress

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 large losses of asset value. The basic function of the payment system is carried out by banks, and monetary policy affects banks 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 for contingencies ranging from pandemic flu to terrorist attacks.

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 et al.) Defense of financial businesses' information systems also helps to deter 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. More recently in 2009, concerns have arisen related to A/H1N1 ("swine") flu. Congress, regulators, and executive branch agencies have responded to each of these threats. This report will be updated as events warrant.

Contents

Appendixes

Contacts

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.[1] 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 and services. They could reduce the pace of economic activity, or at an extreme, cause an actual contraction of economic activity.

It is often argued that the collapse of one prominent entity or interconnected company (such as AIG, Merrill Lynch, or Bear Stearns) could evoke a contagion effect, in which sound financial institutions become viewed as weak, and panicked customers withdraw funds from sound entities, causing sound businesses to fail. Regulators generally address financial problems through deposit insurance and other sources of liquidity (such as emergency loans) for distressed institutions, through safety and soundness regulation, and via direct intervention. One approach is to create special purpose responses to financial stress, such as the Troubled Asset Relief Program (TARP) and Term Asset-Backed Securities Loan Fund (TALF).[2] 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) attempts to 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 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

[1] CRS Report RL32631, *Critical Infrastructure and Key Assets: Definition and Identification*, by John D. Moteff and Paul W. 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 U.S. Department of Homeland Security, The Physical Protection of Critical Infrastructure and Key Assets, at http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf; U.S. Department of Homeland Security, The National Strategy to Secure Cyberspace, at http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf; "Homeland Security Presidential Directive/HSPD-7," at http://www.whitehouse.gov/omb/memoranda/fy04/m-04-15.pdf; U.S. Department of Homeland Security, Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan: Banking and Finance, at http://www.dhs.gov/xlibrary/assets/nipp-ssp-banking.pdf, and U.S. Department of Homeland Security, National Infrastructure Protection Plan: 2009, at http://www.dhs.gov/xprevprot/programs/editorial_0827.shtm.

[2] TARP was authorized by the Emergency Economic Stabilization Act of 2008, P.L. 110-343, and TALF was authorized by the Federal Reserve Act, P.L. 63-43, Section 13(3), as amended.

[3] P.L. 109-144, which expired December 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 RL34219, *Terrorism Risk Insurance Legislation in 2007: Issue Summary and Side-by-Side*, both by Baird Webel.

financial system and the economy.[4] In 2009, TARP was used to provide relief for General Motors and Chrysler.[5]

Pandemic Flu

Recently, the nation has become concerned about the possibility of a pandemic flu outbreak. Large scale illness and quarantines could disrupt the nation's financial system. Proposals have been made to increase teleworking and alternative work locations. The Department of Health and Human Services (HHS) is the lead agency for government planning. It has created a special website that includes a check list for business planning, at http://www.pandemicflu.gov. In addition, the Department of Homeland Security (DHS) has held regional meetings around the nation to encourage businesses and governments to develop contingency plans for possible future disruptions.

Most of 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.

Financial organizations such as the American Bankers Association and the New York Stock Exchange have created the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC), which 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.[6] 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.

In October 2007, FSSCC, Treasury, DHS, and the Securities Industry and Financial Management Association (SIFMA) simulated an influenza pandemic with absenteeism rates reaching 49%.[7] The goals of the exercise were to (1) enhance industry understanding of system risks from flu; (2) provide an opportunity to test plans for a flu pandemic; and (3) 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.

---

[4] CRS Report RL34423, *Government Interventions in Financial Markets: Economic and Historic Analysis of Subprime Mortgage Options*, by N. Eric Weiss.

[5] CRS Report R40003, *U.S. Motor Vehicle Industry: Federal Financial Assistance and Restructuring*, coordinated by Glennon J. Harrison.

[6] FSSCC is discussed in "Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security," below. Patrick McConnell, *Banks and Avian Flu: Planning for a Possible Pandemic*, undated, at https://www.fsscc.org/influenza/banks_and_avian_flu_planning.pdf.

[7] 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.

A Government Accountability Office (GAO) study found that many government agencies would have essential team members telecommute during a pandemic, but that very few had tested their plans.[8]

A flu pandemic is not just a concern of the United States. The International Monetary Fund published a report in 2006 that, in part, addresses the problems that could confront financial institutions.[9] These include continuity of operations, increased delinquency and default on loans due to illness at borrowers' business, and business disruption. The IMF recommended that financial businesses plan 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 using mass transit.

The Role of DHS

The Department of Homeland Security (DHS) is the government agency responsible for communications security oversight.[10] 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.[11] 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.[12] DHS has issued financial institution-specific alerts based on intelligence reports.[13]

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

[8] 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://www.gao.gov/new.items/d06740t.pdf.

[9] International Monetary Fund, *The Global Economic and Financial Impact of an Avian Flu Pandemic and the Role of the IMF*, Feb. 28, 2006 at http://www.imf.org/external/pubs/ft/afp/2006/eng/022806.pdf.

[10] U.S. Department of Homeland Security, *Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan: Communications*, at http://www.dhs.gov/xlibrary/assets/nipp-ssp-communications.pdf.

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

[12] 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.

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

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).

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.[14]

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 healthy banks, otherwise untouched by any cause of failure, are vulnerable to runs in which many depositors seek to withdraw their funds.

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 against collapses of market value—through the Securities Investor Protection Corporation.[15] Each state has a guaranty fund to make good the obligations of 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 ensure that such insurance remains available by protecting providers against catastrophic losses in the event 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.[16] The Federal Housing Finance Agency regulates safety and transparency of important non-depository housing finance institutions.[17] The

[14] CRS Report RS21987, *When Financial Businesses Fail: Protection for Account Holders*, by Walter W. Eubanks.

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

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

[17] CRS Report R40249, *Who Regulates Whom? An Overview of U.S. Financial Supervision*, by Mark Jickling and Edward V. Murphy.

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."[18]

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 consider the inability to process car loans, for example, to be 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 September 11, 2001 terrorist attacks and how the government responded to reduce the chance that the disruption would spread and cause severe finance and economic problems.

Hurricane Katrina

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 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

[18] CRS Report RL34427, *Financial Turmoil: Federal Reserve Policy Responses*, by Marc Labonte.

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, facilitating recovery.[19]

Insurance claims did not threaten the industry. Insured losses from Hurricane Katrina were estimated at $40.6 billion.[20] Nevertheless, the U.S. property-casualty insurance industry's net income after taxes rose by more than 4% during that time.[21] Increasing premiums seem inevitable in affected areas, thereby strengthening industry surpluses and viability.

Blackout of August 14, 2003

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. Although there were isolated problems, the majority of stock, options, commodities, futures, and bond 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.[22]

September 11, 2001

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

[19] CRS Report RS22263, *Katrina's Wake: Restoring Financial Services*, by William D. Jackson and Barbara Miles.

[20] 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/.

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

[22] "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*.)

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. Congress passed the Terrorism Risk Insurance Act (TRIA), at least in part, to encourage insurers to write terrorism risk insurance. Nevertheless, some high-profile commercial properties lack terrorism insurance because of the high cost of such protection in spite of TRIA. The government also provides insurance to domestic airlines under the Air Transportation Safety and System Stabilization Act.[23]

Financial Business Continuity Initiatives

The September 11, 2001 attacks on the World Trade Center temporarily disrupted the nation's financial markets, including the New York Stock Exchange and Cantor Fitzgerald, the company responsible for most of the market for government bonds. 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. The Securities Industry and Financial Markets Association (SIFMA) has created NewBank as a standby to settle Treasury securities trades if one of the two dominant clearing banks were to be unable to perform.[24]

Communications

The Fed, Treasury, and other banking agencies have strengthened their programs for giving financial firms access to priority emergency communications. In the event of a disruption in normal communications, these programs would give priority services to large-value interbank funds transfer, securities pricing and transfer, and payment-related services.

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*.[25] The *Sound Practices* paper covers the largest wholesale financial sector businesses. It does not address retail or trading operations, nor the insurance sector. In April 2006, the three regulatory agencies reported to Congress that the recommendations were substantially in place.[26]

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

[24] Shane Kite, "Bond-Clearing Business Gets Its Backstop," *Securities Industry News*, March 6, 2006.

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

[26] Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency, and Securities and (continued...)

Federal Financial Institutions Examination Council

The Federal Financial Institutions Examination Council (FFIEC) coordinates the examinations by FFIEC's four bank and one credit union regulatory agencies. It has published a public booklet on business continuity planning to assist examiners in evaluation a financial institution's risk management.[27] The booklet provides guidance to the institutions being regulated.

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.[28] Basel II is likely to be revised in light of the financial turmoil that started in 2008.

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

The President appoints executives from 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,

(...continued)

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/fsscc/reports/2006/avian_flu.jsp.

[27] Federal Financial Institutions Examination Council, *Business Continuity Planning*, at http://www.ffiec.gov/ffiecinfobase/html_pages/bcp_book_frame.htm.

[28] CRS Report RL34485, *Basel II in the United States: Progress Toward a Workable Framework*, by Walter W. Eubanks.

[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.

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.

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.[31] Its mission is to coordinate federal and state efforts to improve the reliability and security of the financial system.[32] A public sector group, FBIIC was created by executive order in 2001 and includes representatives of state and national financial and banking regulators.

FBIIC conducts vulnerability assessments of the retail payments 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.[33]

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.[34] 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.

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, that they reopen as quickly as possible. The final element is that resilience requires diversification in case the primary place of business is nonfunctional.[35]

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

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

[33] 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.

[34] 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.

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

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*.[36] The document informs financial firms of national resources available to them.

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

The Financial Services-Information Sharing and Analysis Center (FS-ISAC) has approximately 1,000 members in banking, securities, insurance, and investment. It maintains a database of security threats and system vulnerabilities, which they tie in with the previously noted Treasury bodies.[37] Prominent funds transfer networks and securities exchanges have strengthened their continuity plans both independently and in conjunction with FS-ISAC. 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 by sending out fraudulent emails).[38]

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 others' 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.[39]

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

[36] At https://www.fsscc.org/fsscc/reports/2004/FBIIC_Network_Security.pdf.

[37] "About FS-ISAC," at http://www.fsisac.com/about/.

[38] Financial Services Sector Coordinating Council, *Financial Services Crises Manual of Procedures*, May 3, 2008, at https://www.fsscc.org/fsscc/reports/2008/FS_Crisis_Manual_of_Procedures_ver_1.1.pdf.

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

institutions in the country dealing with strategic approaches to crisis management and payments systems.

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 are banking and financial organizations, some of whom have self-regulatory oversight of their groups, and it covers 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. FSSCC holds meetings with FBIIC.[40]

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.[41]

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.

Department of Homeland Security

Following the attacks of September 11, 2001, Congress created DHS by combining all or part of 22 different agencies.[42] 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.

[40] Financial Services Sector Coordinating Council for Critical Infrastructure, *Sector Specific Plan*, Chapter 5 at https://www.fsscc.org/fsscc/publications/ssp/ssp_5_3.jsp.

[41] ChicagoFIRST, *2008 Annual Report*, at https://www.chicagofirst.org/resources/2008_annual_report.pdf.

[42] 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.

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 since Katrina and have been the basis for planning to mitigate the disruption of a flu pandemic.

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
SIFMA	Securities Industry and Financial Management Association
TRIA	Terrorism Risk Insurance Act of 2002

Author Contact Information

N. Eric Weiss
Specialist in Financial Economics
eweiss@crs.loc.gov, 7-6209

Acknowledgments

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