Order Code RL31873

Homeland Security: Banking and Financial Infrastructure Continuity

Updated December 10, 2004

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

Homeland Security:
Banking and Financial Infrastructure Continuity

Summary

The Department of Homeland Security (DHS) has many responsibilities for ensuring the continuity of the "real" economy: production, distribution, and consumption of public and private goods and services. Other agencies, however, have long had similar responsibilities for the "financial" sectors of the economy, which interact with the sectors DHS oversees pursuant to P.L. 107-296. DHS has some responsibilities for financial sectors, directly and through Treasury Department links. Financial agencies carry out recovery and security activities independently but also coordinately with DHS.

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

Regulators of financial entities have best practice guidelines. The steps include business information technology protocols, physical security protocols, and plans for continuity of markets and participants considered critical for the nation's transactions. Costs of application remain of concern. Further governmental and public-private initiatives have sought to strengthen the resiliency of the financial system's computers, in view of increasing cyberattacks. Many of these arrangements and entities protecting financial institutions against attacks from without are also part of the national effort to prevent terrorist financing within the financial system. (See CRS Report RL32539.) Defenses of financial businesses' information systems are additionally but one of many economy-wide efforts to deter threats to the continuity of American business and government. (See CRS Report RL32331.)

The 107th Congress passed legislation strengthening security for financial institutions and markets. In the 108th Congress, H.R. 657, as passed by the House, sought to strengthen the Securities and Exchange Commission's role in recovery and continuity of securities and related businesses. H.R. 2043 sought to address bank risks under terrorism, among other things. Several hearings examined financial security. Financial sector arrangements appeared among the subjects of Government Accountability Office and 9/11 Commission concerns presented at hearings. The Financial Service Committee's parts of H.R. 10 addressed financial infrastructure concerns. Emergency preparedness in financial infrastructure language was also a carry over from S. 2845 in conference. The final version of the Intelligence Reform and Terrorism Prevention Act of 2004 thus contains requirements in this area that Congress will likely monitor. The act and Members have called for agency and GAO reports on the topic for 2005, suggesting congressional interest ahead.

Contents

Homeland Security: Banking and Financial Infrastructure Continuity

Banking and Financial Institutions Form a Critical Infrastructure

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

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

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

---

[1] CRS Report RL32631, *Critical Infrastructure and Key Assets: Definition and Identification*, by John Moteff and Paul Parfomak.

[2] Congress specified financial services as critical physical and information infrastructure in P.L. 107-56, §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], and "Homeland Security Presidential Directive/HSPD-7", at [http://www.whitehouse.gov/news/releases/2003/12/print/20031217-5.html].

economic effects of either set by acting as lender of last resort to supply liquidity to the financial system, employing monetary policy to expand domestic demand (as it did following the 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. It has done so to prevent troubled entities such as Chrysler, the Farm Credit System, and New York City from defaulting, potentially causing failure in major parts of the financial system and the economy. Collapse of one prominent entity could evoke a contagion effect, in which sound financial institutions become viewed as weak — today's equivalents of a bank run, in which panicked customers withdraw funds from many entities, causing others to fail as well.

The Role of DHS

The Department of Homeland Security (DHS), created by the Homeland Security Act of 2002,[4] has jurisdiction over functions previously assigned to 22 agencies with respect to certain communications, transportation, and computer ("cyber") security. These are essential parts of the physical infrastructure upon which the financial system relies as a user. They are also parts of the electronic infrastructure of information storage, retrieval, and transmission. The heart of financial services is information that providers transform into useful forms, such as account balances at banks, securities price quotations, executions of purchase and sales of financial assets, and payments on contractual obligations such as loans.

Although networks of communication are vital to their work, financial services companies do not generally maintain communications and transportation networks, nor design software or manufacture hardware and carriage devices such as airplanes and trucks. Security of communication thus resides with sectors covered by DHS.[5] Financial institutions and their regulators operate in a different environment than nonfinancial ones: they have been developing appropriate (sometimes different) security protocols within existing frameworks.

As noted below, however, DHS interacts with Treasury Department bodies concerned with financial security. The need for combined cybersecurity for data and physical operations of financial businesses, interconnected via the Internet and otherwise, had received the attention of the former federal Critical Infrastructure Assurance Office.[6] And, the Treasury has agreed with DHS to assign an expert in financial services matters to DHS. Eventually, DHS will rotate experts from other

---

[3] P.L. 107-297, Title III, Nov. 26, 2002.

[4] P.L. 107-296, Nov. 25, 2002.

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

[6] Marcia Kass, "Business Continuity, Solutions Integration Highlight Homeland Security Conference," *BNA's Banking Report*, Dec. 16, 2002, p. 969.

financial regulators into the position.[7] Following its move into DHS, the Secret Service, in cooperation with the Carnegie Mellon Software Institute, has studied threats to information systems in critical financial infrastructures.[8] DHS also issued financial institution-specific alerts in 2004, based on intelligence reports.[9]

Safety Net Measures in Place

Financial Risks

Financial regulation includes deposit insurers, safety and soundness regulators throughout the financial sectors, and the Fed as lender of last resort and ultimate protector of the financial system. A multiplicity of arrangements protects financial institutions and their customers from many kinds of collapse.[10]

The Fed has long stood ready to provide liquidity to the banking system. The Federal Deposit Insurance Corporation (FDIC) protects depositors against failure of a bank or savings association. It helps guard against depositor panics that drain banks of their funds and create a severe liquidity crisis as they curtail lending, or call in loans to meet deposit withdrawals. Even a healthy depository institution, otherwise untouched by any cause of failure, would not long withstand a depositor panic. The FDIC brings order to the process of resolving such a financial failure. This agency has long had authority to prevent the failure of a bank it deems essential, which Congress supplemented in the 1980s and 1990s to allow even greater flexibility. The FDIC may borrow up to $30 billion from the U.S. Treasury, if needed for rescue operations. Credit unions have similar arrangements with their Central Liquidity Facility and Share Insurance Fund. Observers often regard pension funds as separate financial institutions with identified balances of each account-holder. Society federally supports certain pension funds, those with defined benefits, as well by the Pension Benefit Guaranty Corporation.

Although the securities industry lacks a pool of emergency liquidity, securities firms may also borrow from the Fed if it allows them. Government protects individual securities accounts against operational losses — although not collapses of market value — through the federally-sponsored Securities Investor Protection Corporation. All states have guaranty funds to make good the obligations of their

---

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

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

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

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

state-regulated insurance companies in case of insolvencies, although, again, no pool of liquidity exists for most of this industry nationally. TRIA provides a federal backstop for insurers willing to provide terrorism insurance. Congress intended this law to assure that such insurance remains available, while protecting providers against catastrophic payouts in case of terrorist attacks.

Other agencies bolster the national financial safety net by seeking to maintain confidence in other ways. A multiplicity of entities and processes are part of the ongoing safety net, although they do not necessarily assure liquidity or rescue of a financial failure. For many years, the securities industry and securities issuers have had overseers and programs designed to prevent against collapse of confidence originating within the system. The Securities and Exchange Commission (SEC), directly and through industry-based self-regulatory organizations such as stock exchanges, and accountancy standards, has sought transparency ("disclosure") in financial practices, and trading in public securities, of businesses. The Sarbanes-Oxley Act of 2002[11] sought further to restore investor confidence by strengthening accountability for Corporate America. Both the Federal Housing Finance Board and the Office of Housing Enterprise Oversight (OFHEO) regulate safety and transparency of important non-depository housing finance institutions. The Commodity Futures Trading Commission (CFTC) oversees organized markets on futures and similar contracts, through self-regulatory organizations.

Every state has one or more regulatory bodies responsible for state-chartered banks, credit unions, thrift institutions, and companies engaged in securities and futures operations. Although state-chartered depository institutions are subject to much federal regulation, the states alone primarily regulate insurance companies, finance companies, mortgage bankers, and the like. All 50 states oversee industry-funded guaranty funds to cover insolvencies in insurance companies, and some sponsor insurance for credit unions. State regulatory bodies for their respective industries are linked via 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. The Fed has statutory authority to lend to businesses directly in "unusual or exigent circumstances," which Congress strengthened in TRIA.[12]

---

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

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

Operational/Security Risks

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

Safety and Continuity in Recent Experience

Last Decades of 1900s. Sudden drops in the value of financial assets have affected the U.S. financial system late in the 20th century, including the stock market's crash in 1987, the savings and loan/banking collapse of 1989-1991, the Gulf War shock of 1991, and the Asian/Russian financial crises of 1997-1998. The Fed and other financial regulators took positive steps to alleviate the resulting difficulties, providing liquidity to the banking system, and therefore to the economy. They then planned steps that in hindsight might have cushioned against experienced collapses of value. Following the stock market plunge in 1987, the President's Working Group on Financial Markets[13] issued recommendations, many of which became practice. That group resurfaced after the late-1990s international disturbances that threatened the U.S. through just one investment fund: Long Term Capital Management. It examined problems that certain derivatives posed to the economy in 1999. Congress passed reforms of federal deposit insurance and banking regulators' authorities over practices threatening depository institutions generally in 1989 and 1991.[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.

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

2001. With the September 2001 destruction of the World Trade Center, both problems — financial loss of asset values, and operational interruption — occurred

---

[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.

simultaneously. The financial side of the response worked well, as the Fed provided the necessary liquidity to prevent panic. It injected $80 billion, then more, into the banking system. It arranged international facilities to keep financial economies operating globally. The Fed and other central banks cut interest rates worldwide, to ease pressures on borrowers. Its stimulus may have exceeded $300 billion.

The SEC issued emergency rules encouraging buying in the stock market once it reopened. Trading recommenced rapidly, as the U.S. Treasury security market opened on September 13, and the equities market was in full operation by September 17. Physical infrastructure recoveries took a few days of heroic efforts (e.g., running new connections into Manhattan). Off-site record keeping, sharing of working space with displaced competitors, and increasing reliance on electronic tracing and communications systems by institutions outside the attack area, allowed for resumption of near-normal operations quickly. Nonetheless, regulators and industry groups made it known that financial firms would need new contingency plans and stress tests to protect against more extreme situations in the future. Many insurance companies ceased protecting against terrorist-related claims or raised premiums for such coverage sharply. Operators of high-profile commercial properties now often go without terrorism indemnity, since high prices still accompany federally-supported coverage, as noted above. The government also provides insurance to domestic airlines under the Air Transportation Safety and System Stabilization Act.[15]

Blackout of 2003/Hurricanes of 2004. Emergency response measures noted above helped reduce the financial market damages from a massive August 14 power blackout in the northeastern United States and Canada. The Treasury Department received no reports of major disruptions or losses of financial data, in large part because of steps taken to make systems resilient and redundant. Despite glitches, the major markets, in stocks, options, commodities, futures, and bonds, were soon open. Banks closed affected offices, in New York and Detroit; otherwise, the banking system overwhelmingly stayed open. The Fed's payments and emergency lending to banks systems operated well. Banks borrowed $785 million from the Fed after the blackout, the most since $11.7 billion of the week after 9/11,and have since repaid these amounts. New applications for mortgages did fall temporarily because of the blackout. Contrary to initial fears, terrorists had not caused the blackout and thus it did not severely stress the financial economy.[16]

Several financial institutions in the southern/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, after the fact. They have since resumed operations, despite physical damage. The

---

[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," Ibid., Aug. 18, 2003.

insurance industry, faced with large payouts for storm-related damage to many sectors, seems likely to rebound.

Financial Business Continuity Proposals

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

Regulatory

Government Securities Clearing. Regulators are concerned about the U.S. government securities market, in view of its critical role for conducting monetary policy operations, financing government activities, and providing benchmark prices and hedging opportunities for other securities markets. On May 13, 2002, the Fed, the OCC, and the SEC issued a White Paper on Structural Change in the Settlement of Government Securities. That paper expressed concerns about operational, financial, and structural vulnerabilities from having only two clearing banks. In response, the Fed will initiate a back-up "dormant" clearing and settlement bank, ready to act should the two banks clearing government securities be unable to do so, and other mitigatory measures.[17] One of them experienced massive computer failure preventing this market from functioning, decades ago.[18]

Communications. At the intersection of financial and communications markets, the Fed (in coordination with Treasury and the other banking agencies) has strengthened its programs for giving financial businesses emergency preparedness access to priority communications.[19] These programs, which the National Communications System administers, help financial markets facing substantial operational disruptions. They are (1) Telecommunications Service Priority for circuits used in large-value interbank funds transfer, securities pricing and transfer, and payment-related services; (2) Government Emergency Telecommunications

---

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

[18] U.S. Congress, House, Committee on Banking, Finance, and Urban Affairs, Subcommittee on Domestic Monetary Policy, *The Federal Reserve Bank of New York Discount Window Advance of $22.6 billion Extended to the Bank of New York* (Washington: GPO, 1986).

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

Service (GETS) for priority processing of 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 through low-cost cards.[20]

Interagency Paper on Sound Practices. The Fed, the OCC, and the SEC have issued an "Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System."[21] This final regulation, which applies most directly to the clearing and settlement activities of a few financial institutions, provides some flexibility to firms in managing geographic dispersion of backup facilities and staffing arrangements, and takes into account cost-effective application of sound practices. It includes participation from the New York State Banking Department and the Federal Reserve Bank of New York.[22]

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

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

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

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

---

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

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

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

FFIEC. The four bank and single credit union regulatory agencies, however, meet together as the Federal Financial Institutions Examination Council. This Council's information technology subcommittee serves as a vehicle for coordinating agency policies on technological and related risks now including security protocols and financial business continuity.[23] It is coming to have a larger role in physical- and cyber-security financial protocols.

Basel II. For the largest U.S. commercial banking organizations, the Fed has proposed additional mandates in its planned regulation known as the"Basel II Capital Accord." Among the issues raised by Basel II is its controversial operational risk requirement for covered firms to carry greater capital. Operational risk refers to noncredit risk factors including system failures and terrorism. Hearings by two subcommittees of the House Financial Services Committee in 2003 explored some of its implications, which most bankers feel are burdensome.[24] The 108th Congress measure, United States Financial Policy Committee for Fair Capital Standards Act, H.R. 2043, addressed Basel II, including its operational risk component.

Fed Rescue Plan. In the broader picture, the Fed was reportedly planning to lend massively to banks and other entities to ensure that financial markets do not lock up, should another major shock occur against the financial system. It may attempt such a rescue plan for the economy — even without another 9/11 emergency.[25]

Executive

Government's Own Financing. Congress generally requires financial bodies within government itself to develop, document, and carry out agency-wide information security programs under the E-Government Act of 2002.[26] The Treasury Department and other federal bodies have taken steps to protect the government's critical financial functions including to borrow; make payments including social security; and raise revenue through the Internal Revenue Service. Should the threat level rise, agencies will (1) increase physical and cyber-security measures including security forces, the frequency of security patrols, identity checks, and restricting access with state and local authorities to enhance physical security for specific assets; (2) disperse individuals critical to operations; and (3) use backup facilities.[27]

---

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

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

[25] "Fed Piecing Together Emergency Economy Plan," *Wall Street Journal Online*, Apr. 7, 2003; and "Fed Ferguson Says Emergency Econ Rescue Plan Exaggerated," ibid., Apr. 8, 2003.

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

[27] "Treasury Statement on Measures to Protect the Financial Markets during (continued...)

Presidential. President Bush has appointed executives of the banking and securities industries to the National Infrastructure Advisory Council (NIAC). The members of this panel advise the White House on cyber- and information-security of critical economic infrastructures, including financial ones. It builds upon, in part, the former Critical Infrastructure Assurance Office created in 1998 to coordinate federal initiatives on critical infrastructures. Members of NIAC represent major sectors of the economy — banking and finance, transportation, energy, information technology, and manufacturing. It also includes representatives from academia, state and local government, and law enforcement. NIAC works closely with the President's National Security and Telecommunications Advisory Committee.[28]

NIAC meets periodically to:

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

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

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

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

(v) advise lead agencies with critical infrastructure responsibilities, sector coordinators, DHS, and ISACs, including for the banking and finance sector.[29]

FBIIC. Treasury's Office of Critical Infrastructure Protection, formed after 9/11, under Treasury's Office of Financial Institutions, staffs the Financial and Banking Information Infrastructure Committee (FBIIC). Its chair is the Treasury's Assistant Secretary for Financial Institutions.[30] Its mission involves coordinating federal and state efforts to improve the reliability and security of the financial system.[31] FBIIC, created by executive order in 2001, includes representatives of the:

---

[27] (...continued)
Hostilities with Iraq," Mar. 17, 2003, at [http://www.treas.gov/press/releases/js114.htm].

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

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

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

[31] Financial and Banking Information Infrastructure Committee, "FBIIC," at [http://www.fbiic.gov].

— Commodity 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
— Homeland Security Council
— 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
— Office of Federal Housing Enterprise Oversight
— Office of Thrift Supervision
— Securities and Exchange Commission
— Securities Investor Protection Corporation.

FBIIC is to (1) identify critical infrastructure assets, their locations, potential vulnerabilities, and rank their importance to the financial system of the United States; (2) secure communications capability between the financial regulators and protocols for communicating during an emergency; and (3) ensure sufficient staff at each member agency with appropriate security clearances to handle classified information and coordinate in case of an emergency. FBIIC will conduct vulnerability assessments of the retail payment system, government-sponsored enterprises, and the insurance industry — none directly addressed in the White Paper noted above — and other improvements to financial resiliency.[32] Along these lines, the Treasury has formulated procedures for securing communications between federal and state financial regulators to share information about an event affecting their regulated financial institutions.[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

---

[32] 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].

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

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

communication for market participants. The department has also offered to provide secret physical security measures to key financial institutions requesting them.[35]

A more concrete outline of Treasury's approach to the problems is its four-pronged overall approach to promoting continuity in the financial system and preventing interruption in case of a catastrophe. The focus first is on people. The second critical element is maintaining a high level of confidence in the functioning of the financial system. The third element is making sure that markets remain open — or, if they do close, reopen as quickly as possible. The final element is that resilience requires diversification if the primary place of business is nonfunctional.[36]

In a specific cooperative modality, the Treasury has created a Protective Response Planning Program. This program brings together federal and local government officials, members of law enforcement and individuals from important financial institutions to develop and coordinate emergency responses to major disruptions at these specific institutions.[37]

OFHEO. Disaster recovery and back-up protocols mentioned in the Interagency Paper are seemingly also required by OFHEO — an independent office within the Department of Housing and Urban Development — in its safety and soundness examinations of the troubled government-sponsored housing finance enterprises it oversees. The latter, the Federal Home Loan Mortgage Corporation and Federal National Mortgage Association, are developing resilience internally as well.[38]

Department of Justice. Independently of other efforts, this Department has promulgated a set of "Suggested Best Practices on Internet and Computer Security for Financial Institutions." The document informs financial firms of national resources available to them as well.[39]

Private Sector

FS-ISAC and Payments Networks. Y2K and other threats to financial companies had been feared for years. Many businesses sought to defend their operations in advance through hardware and software tests and upgrades. For example, they created the Financial Services Information Sharing and Analysis Center (FS-ISAC) in 1999. The nation's largest banking, securities, insurance, and investment firms participate in FS-ISAC, maintaining a database of security threats

---

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

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

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

[38] Communication from Peter Brereton of OFHEO to William Jackson, Apr. 3, 2003.

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

and system vulnerabilities, which they tie in with Treasury's bodies noted above.[40] Participants privately run FS-ISAC, like ISACs of 14 sectors. Among its other accomplishments, 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."[41] The Treasury Department has awarded a $2 million contract to it to upgrade financial institution security and to increase its membership beyond the 50-plus largest critical firms.[42] Prominent funds transfer networks and securities exchanges have strengthened their continuity plans both coordinatively with, and independently of, FS-ISAC.[43] The organization has 870 direct members, with about ten times that number indirectly through associations, and is actively seeking new members with federal encouragement.[44]

Securities Industry. The Securities Industry Association (SIA) has released best practices guidelines for its members' recovery from disasters. SIA is also working with utility providers in New York to improve physical recovery measures. The New York Stock Exchange has developed back-up and redundancy facilities, although terror attacks did not damage its own facilities. This exchange and the over-the-counter NASDAQ have agreed to trade each other's stocks if either were to become incapacitated. The National Association of Securities Dealers may require business continuity plans of a similar nature. Measures revealed by the industry include that most securities firms created backup sites far from New York, as the Interagency Paper suggested, and wired a network to the Stock Exchanges through Consolidated Edison's underground pipes.[45]

Banking Industry. As was noted above, extensive regulatory and supervisory protocols apply to banks as businesses. The potential for targeted cyber-disruption exists even for single banking firms. In 2003, the "SQL Slammer" worm shut down Bank of America Corp.'s Automated Teller Machines. Two large U.S. banks shut down their Machines after discovering that the "Welchia/Nochi" worm had attacked them.[46] Organizations such as "BITS," the technology arm of the Financial Services

---

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

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

[42] U.S. Treasury Department Press Release, Dec. 9, 2003, at [http://www.treas.gov/press/releases/js1047.htm].

[43] 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].

[44] Hannah Bergman, "A Push for Disaster Recovery Programs," *American Banker Online*, Dec. 3, 2004.

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

[46] David Breitkopf, "Worms, Crawling Through Windows, Menace ATMs," (continued...)

Roundtable trade group, focus on industry defenses. BITS estimates that bankers collectively spend more than $1 billion on technology to mitigate cyber-threats annually. Daily patches are becoming industry practice. [47] Bankers may also purchase some insurance against liability for loss of customer confidential information through hacking, transmittal of a virus to customers from bank websites, and denial of access when customers are unable to get to information because bank servers are down.[48]

FSSCC. Organizations representing most significant financial entities have joined the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security.[49] Its members, some of whom have self-regulatory oversight of their groups, cover most of America's finance. Members are the:

— American Bankers Association
— America's Community Bankers
— American Council of Life Insurers
— American Society for Industrial Security
— Bank Administration Institute
— BITS and Financial Services Roundtable
— Chicago First
— Chicago Mercantile Exchange
— Consumer Bankers Association
— Credit Union National Association
— Depository Trust and Clearing Corporation
— Fannie Mae
— Financial Services Information Sharing and Analysis Center
— 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) Clearing House
— Securities Industry Association
— Securities Industry Automation Corporation
— Bond Market Association

---

[46] (...continued)
American Banker Online, Dec .10, 2003.

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

[48] Lee Ann Gjertsen, "St. Paul Web-Risk Policy Offers Small-Bank Shield," Ibid., Nov. 7, 2003.

[49] "Information," at [http://www.fsscc.org/].

— Options Clearing Corporation
— VISA USA Inc.

This body coordinates regularly and voluntarily with FBIIC.

Congressional

Post-9/11 Legislation. The 107th Congress passed TRIA to backstop terrorism insurance for property-casualty insurers and airlines. Application of such aid continues. Other congressional measures, including tax relief for investors and financial integrity initiatives, seemingly increased confidence in the securities markets by 2003. The House approved a bill to give the SEC additional authority in case of a national emergency, on February 26, 2003. This Emergency Securities Response Act, H.R. 657, 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.

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

In the first study, GAO recommended that the Treasury Department coordinate with the banking and finance industry to update the sector's National Strategy for Critical Infrastructure Assurance and to improve the process for monitoring its progress. GAO suggested Treasury assess the need for grants, tax incentives, regulation, or other public policy tools.[50] GAO found deficiencies in the Treasury/Federal Reserve Internet payments system known as "pay.gov," which seem to have been fixed.[51]

---

[50] 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].

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

Congress examined the agency's second set of findings[52] in a House Financial Services Subcommittee on Capital Markets, Insurance and Government Sponsored Enterprises hearing held February 12, 2003.[53] GAO found that the Fed; the regulator of national banks, the Office of the Comptroller of the Currency (OCC); and SEC lack a strategy for having their regulatees resuming trading in securities following any future disruption of the financial market, and should work with industry to develop a plan. GAO's most direct recommendation for actions were primarily for the SEC's operations risk oversight. For bank regulation, GAO noted that examiners review physical security, but do not generally focus on terrorism mitigation.

In a surprising finding, GAO's study of the Treasury's own information technology protocols found that the Department's chief information officer needed to improve Department-wide financial information security controls.[54]

GAO performed a follow-up study of its 2003 findings, released in 2004.[55] Examining five broker-dealers and three large banks, the agency concluded that they had done much to reduce risks, including beefing up physical and technical security. Despite earlier recommendations, four of the eight companies still had all of their critical trading staff in one location, by that leaving markets without adequate liquidity for fair and efficient trading in case of catastrophes. It recommended that the SEC improve information technology oversight and analyze the ability of securities markets to recover from a major disruption. SEC Chairman Donaldson agreed with the recommendations and said the SEC was addressing them.[56]

Members requested that GAO submit an additional follow-up study during 2005.

---

[52] It is available in three versions: 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].

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

[54] U.S. Government Accountability Office, *Improvements Needed in Treasury's Security Management Program*, GAO-04-77.

[55] U.S. Government Accountability Office, *Financial Market Preparedness: Improvements Made, but More Action Needed to Prepare for Wide-Scale Disasters*, GAO-04-984.

[56] Hannah Bergman, "In Brief: Trading Firms Unready for Terror Attack," *American Banker Online*, Oct. 28, 2004.

Intelligence Reform and Terrorism Prevention Act of 2004

Beyond anti-terrorist tactics and financing legislative recommendations, the 9/11 Commission findings of 2004 evoked major financial preparedness legislation. Congressional followup, H.R. 10, received Committee on Financial Services attention. Its markup amendments strengthened financial institutions from within, against natural and unnatural (terrorist) disasters in their operations, among many other things. The Senate counterpart, S. 2845, was silent on these matters.

Following a conference, the resulting Intelligence Reform and Terrorism Prevention Act of 2004 places requirements on the Departments of Homeland Security and Treasury. In §7306, DHS is to report on vulnerability and risk assessments and the government's plans to protect infrastructures, including financial institutions. The rest of required legislated preparedness rests upon the shoulders of Treasury. §6303 requires a Treasury report on "the effectiveness and efficiency of efforts to protect the critical infrastructure of the United States financial system . . . " §7802 requires the Treasury to report on its efforts to encourage public/private partnerships to protect critical financial infrastructure. §7803is titled "Emergency Securities Response Act of 2004." It enables the SEC to issue orders and take other emergency actions to address extraordinary private securities market disturbances. The agency is to consult with Treasury, the Fed, and the Commodity Futures Trading Commission before acting. It grants Treasury authority parallel with that of the SEC for government securities market disturbances. §7803 additionally requires the Fed, the Office of the Comptroller of the Currency, and the SEC to report on private sector financial business continuity plans, including more financial services entities than are under existing regulation. The agencies published their regulation in the *Federal Register* as the *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*, noted above. §7804 expresses the sense of Congress that insurance and credit rating companies consider businesses' compliance with private sector standards in assessing insurability and creditworthiness, to encourage private sector investment in disaster and emergency preparedness.

Thus, the enacted measure would increase governmental and private emergency preparedness planning. It would encourage financial businesses smaller than the largest "wholesale" transacting and clearing entities, the only firms now covered by the *Interagency Paper*, to undertake emergency preparedness. The insurance and credit rating provision resembles concerns over lending and insuring in areas subject to flooding and the like, where planning against consequences of disasters is highly relevant. Its requirements for reports to Congress in 2005 most likely will involve oversight hearings.

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

Many practices in the *Interagency Paper* came from financial firms' experiences and may thus be considered both public and private-sector ideas. Should the threat level increase, government expects critical private financial institutions to have security forces, identity checks, and restricted access, and to work with state and local

authorities.[57] The Fed, a body with both public and private elements,[58] remains ready to be the lender of last resort to the financial system and its customers as well. Recovery in the blackout of 2003, for example, was helped by the Fed, institutions activating internal contingency plans, and a paging and alert system set up after 9/11 by the Financial Services Roundtable (a group of major financial providers) and its technology arm BITS.[59]

List of Major Acronyms

CFTC	Commodity Futures Trading Commission
DHS	Department of Homeland Security
FBIIC	Financial and Banking Information Infrastructure Committee
FDIC	Federal Deposit Insurance Corporation
Fed	Federal Reserve System
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
OFHEO	Office of Housing Enterprise Oversight
SEC	Securities and Exchange Commission

---

[57] "Treasury Statement on Measures to Protect the Financial Markets during Hostilities."

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

[59] Blackwell, "Backup Site Questions."

The security level of financial applications is improving. The percentage of e-banking systems with critical vulnerabilities has tended to fall in recent years. Critical vulnerabilities were detected in 90 percent of systems in 2015, 71 percent in 2016, and only 56 percent in 2017.Â This year, financial applications based on ready-made vendor solutions contained fewer critical vulnerabilities than in-house applications. Vendors have started to pay more attention to security issues, while banks still lack experienced developers and a mature Secure Software Development Lifecycle (SSDLC). In 2017, the majority of analyzed systems (61%) were in production and accessible to clients. How was the Office of Homeland Security established? through executive order. 5 basic responsibilities of the Office of Homeland Security. 1. Work with federal, state, and local agencies to prepare for a possible terrorist event. 2. Mitigate the consequences of threats and attacks.Â 4. Protect critical infrastructure from terror attacks. 5. Provide incident management, continuity of government, and public education on terrorism. Who was chosen to run the Office of Homeland Security? Former PA Governor Tom Ridge. When was the Department of Homeland Security created? 2002.Â ICE Homeland Security Investigations. Financial crimes, money laundering, and bulk cash smuggling. Commercial fraud and intellectual property theft. Cybercrimes. Treasury and Homeland Security are working with the financial sector, academia, and other government agencies to focus on cyber security concerns. The information security industry has grown rapidly to mitigate risks by providing a myriad of products and services, including firewalls, access controls, anti-virus and anti-spyware programs, audits, standards (e.g., Common Criteria), and software patches.Â The Banking and Finance Sector relies on an information technology infrastructure, including computing hardware, software, and telecommunications networks. Some of this infrastructure is owned and operated by financial institutions and some is provided by third party service providers in the US and around the globe. Jackson, W.D.: Homeland security: banking and financial infrastructure continuity, CRS Report for Congress (2004) Google Scholar. 6. Bologna, S., Setola, R.: The need to improve local self-awareness in CIP/CIIP.Â PCI Security Standard Council, Payment Card Industries (PCI): Data Security Standard Requirements and security assessment procedures. Available online at: https://www.pcisecuritystandards.org/security_standards/download.html?id=pci_dss_v1-2.pdf. 12. Sommerville, I.: Software Engineering. Addison-Wesley, Reading (2001) Google Scholar. 13. Federal Financial Institutions Examination Council (FFIEC): Information Security Booklet, Information Technology Examination Handbook (2006) Google Scholar. â€¢ Improve resilience of the telecommunications infrastructure supporting critical financial services. Some of the key steps the Federal Reserve has taken to improve our infrastructure and the delivery of critical central-bank and financial services include the following: â€¢ We have developed plans to ensure that critical central-bank activities, supervisory functions, and financial services operations have sufficient redundancy in facilities and staff. We have enhanced and tested business-continuity arrangements for critical functions and business lines. â€¢ Our facilities for providing critical