United States Government Accountability Office

GAO

Report to Congressional Requesters

October 2009

INFLUENZA PANDEMIC

Key Securities Market Participants Are Making Progress, but Agencies Could Do More to Address Potential Internet Congestion and Encourage Readiness

GAO

Accountability * Integrity * Reliability

GAO-10-8

October 2009

GAO
Accountability • Integrity • Reliability

Highlights

Highlights of GAO-10-8, a report to congressional requesters

INFLUENZA PANDEMIC

Key Securities Market Participants Are Making Progress, but Agencies Could Do More to Address Potential Internet Congestion and Encourage Readiness

Why GAO Did This Study

Concerns exist that a more severe pandemic outbreak than 2009's could cause large numbers of people staying home to increase their Internet use and overwhelm Internet providers' network capacities. Such network congestion could prevent staff from broker-dealers and other securities market participants from teleworking during a pandemic. The Department of Homeland Security (DHS) is responsible for ensuring that critical telecommunications infrastructure is protected.

GAO was asked to examine a pandemic's impact on Internet congestion and what actions can be and are being taken to address it, the adequacy of securities market organizations' pandemic plans, and the Securities and Exchange Commission's (SEC) oversight of these efforts. GAO reviewed relevant studies, regulatory guidance and examinations, interviewed telecommunications providers and financial market participants, and analyzed pandemic plans for seven critical market organizations.

What GAO Recommends

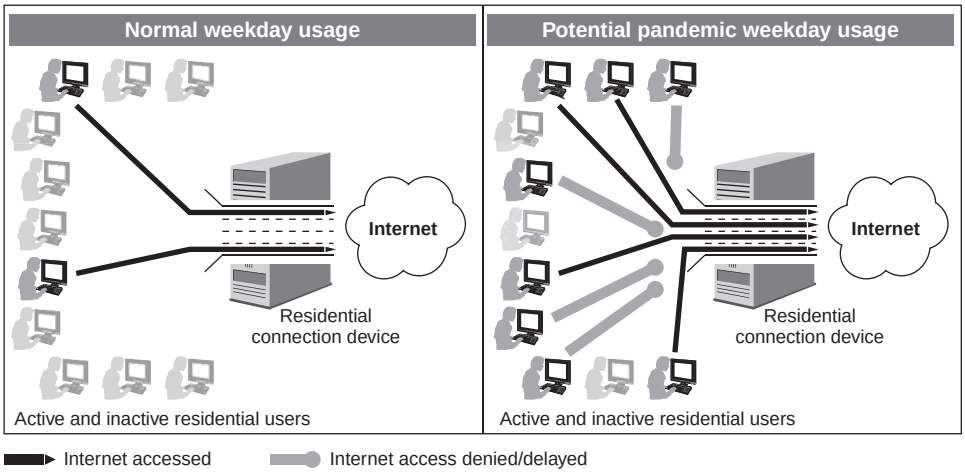
GAO recommends DHS begin planning to address Internet congestion and SEC better review market participants' plans. SEC agreed. DHS agreed to address potential congestion for national security and emergency communications, but not more broadly. GAO believes DHS should do more to address potential Internet congestion.

View GAO-10-8 or key components.
For more information, contact Mathew J. Scirè at (202) 512-8678 or sciremj@gao.gov

What GAO Found

Increased demand during a severe pandemic could exceed the capacities of Internet providers' access networks for residential users and interfere with teleworkers in the securities market and other sectors, according to a DHS study and providers (see figure below). Private Internet providers have limited ability to prioritize traffic or take other actions that could assist critical teleworkers. Some actions, such as reducing customers' transmission speeds or blocking popular Web sites, could negatively impact e-commerce and require government authorization. However, DHS has not developed a strategy to address potential Internet congestion or worked with federal partners to ensure that sufficient authorities to act exist. It also has not assessed the feasibility of conducting a campaign to obtain public cooperation to reduce nonessential Internet use to relieve congestion. DHS also has not begun coordinating with other federal and private sector entities to assess other actions that could be taken or determine what authorities may be needed to act.

Likely Internet Congestion Points Affecting Teleworkers



Source: GAO.

Because the key securities exchanges and clearing organizations generally use proprietary networks that bypass the public Internet, their ability to execute and process trades should not be affected by any congestion. In analyzing seven critical market organizations, GAO found they had prepared pandemic plans that addressed key regulatory elements, including hygiene programs to minimize staff illness and continuing operations by spreading staff across geographic areas. However, not all had completed or documented analyses of whether they would have sufficient staff capable of carrying out critical activities if many of their employees were ill. Also, not all had developed alternatives to teleworking if congestion arises. SEC staff have been regularly examining market organizations' readiness, but could further reduce risk of disruptions by ensuring that these organizations prepare complete staffing analyses and teleworking alternatives.

Contents

Letter 1

Background 3
Internet Congestion During a Severe Pandemic That Hampers Teleworkers Is Anticipated, but Responsible Government Agencies Have Not Developed Plans to Address Such Congestion and May Lack Clear Authority to Act 14
Key Securities Market Participants Have Prepared Response Plans, but Not All Have Documented Staffing Analyses or Plans for Alternatives to Teleworking 29
SEC Has Taken Significant Steps to Assess Securities Market Organizations' Pandemic Preparedness, but Could Do More 40
Conclusions 45
Recommendations for Executive Action 47
Agency Comments and Our Evaluation 47

Appendix I **Objectives, Scope, and Methodology** 52

Appendix II **FINRA Efforts to Oversee Pandemic Readiness of Broker-Dealers** 55

Appendix III **Steps Taken by Bank Regulators to Assess Pandemic Preparedness in Key Clearing Banks** 59

Appendix IV **Comments from the Securities and Exchange Commission** 61

Appendix V **Comments from the Department of Homeland Security** 63

Appendix VI **GAO Contacts and Staff Acknowledgments** 71

Figures

Figure 1: Overview of the Internet 7
Figure 2: Role of Various Securities Market Participants in a Typical Securities Trade 9
Figure 3: Potential Points of Congestion 16

Abbreviations

ARP	Automation Review Program
CMTS	cable modem termination system
CDC	U.S. Centers for Disease Control and Prevention
DHS	Department of Homeland Security
DSL	digital subscriber line
DSLAM	digital subscriber line access mutiplexer
FBIIC	Financial and Banking Information Infrastructure Committee
FCC	Federal Communications Commission
Federal Reserve	Board of Governors of the Federal Reserve System
FINRA	Financial Industry Regulatory Authority
FS/ISAC	Financial Services Information Sharing and Analysis Center
FSSCC	Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security
GETS	Government Emergency Telecommunications Service
HHS	Department of Health and Human Services
HSPD-7	Homeland Security Presidential Directive 7
IT	information technology
Mbps	megabits per second
NCS	Office of the Manager of the National Communications System
NS/EP	national security/emergency preparedness
PSA	public service announcement
TSP	Telecommunications Service Priority Program
SEC	Securities and Exchange Commission
Treasury	Department of the Treasury
WHO	World Health Organization

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

October 26, 2009

Congressional Requesters:

The outbreak of the H1N1 flu in April 2009, while not as severe as initially expected, has underscored the concerns that a potentially serious virus could emerge that would cause widespread illness and deaths. U.S. health authorities have estimated that a pandemic similar to the one that occurred in 1918 could sicken millions of people in the United States and potentially cause many deaths. The impact of such an event on various sectors of the U.S. economy could also be significant. In a severe pandemic, governments may close schools, shut down public transportation systems, and ban public gatherings such as concerts or sporting events. In such scenarios, many more people than usual may be at home during the day, and Internet use in residential neighborhoods could increase significantly as a result of people seeking news, entertainment, or social contact from home computers. Concerns have been raised that this additional traffic could lead to congestion on the Internet that would significantly affect businesses in local neighborhoods, such as small doctors' offices or business employees attempting to telework by connecting to their employers' enterprise networks.

Among the organizations that could be affected by potential pandemic-related Internet congestion are those participating in the U.S. securities markets. For these markets to function, various organizations must be able to operate, including the exchanges or electronic trading venues that execute the orders received from broker-dealers. After trades are executed, a clearing organization processes the information to verify the accuracy of the transaction and to transfer ownership of the securities from the seller to the buyer. Payments are also transferred among the banks used by clearing organizations and broker-dealers by various payment processors. We have previously issued a series of reports on the progress that the various organizations participating in the securities markets have made in preparing their organizations to prevent various threats—such as physical or cyber attacks—from disrupting their

operations.[1] Although many organizations participate in U.S. securities markets, the amount of trading volume or importance of the role played by certain of these exchanges, clearing organizations, or payment processor organizations is such that if one was not able to continue operating after a disaster, the ability of the overall markets to function could be affected.

In asking us to review the potential impact of Internet congestion that arises during a severe pandemic, you raised questions about whether such congestion could significantly affect the ability of securities market participants to continue operating effectively, including by using teleworking, during a pandemic. In this report, we address (1) the potential impact of a severe pandemic on the Internet and the actions telecommunications providers and government agencies are taking to address possible congestion, (2) the adequacy of the actions that securities market organizations are taking to prepare pandemic plans, and (3) steps that securities and other regulators are taking to assess the readiness of securities market organizations to continue operating during a pandemic.

To address these objectives, we reviewed relevant studies and discussed network capacities and capabilities with four major Internet providers that provide service to a large part of the United States, including many major cities. We also interviewed officials from federal agencies responsible for telecommunications and pandemic issues, including the Federal Communications Commission (FCC), the Department of Homeland Security (DHS), and the Department of Health and Human Services (HHS). We reviewed the pandemic plans and other related documents from the same seven critical securities market organizations covered in our prior reports—including key exchanges, clearing organizations, and payment processors—whose operations are more critical to the overall functioning

[1]In the aftermath of the September 11, 2001 attacks, we conducted a series of reviews that examined the steps being taken by securities market participants to improve their physical security, information security, and business continuity capabilities. See GAO, *Potential Terrorist Attacks: Additional Actions Needed to Better Prepare Critical Financial Market Participants*, GAO-03-251 (Washington, D.C.: Feb. 12, 2003); *Potential Terrorist Attacks: Additional Actions Needed to Better Prepare Critical Financial Market Participants*, GAO-03-414 (Washington, D.C.: Feb. 12, 2003). These reports were addressed to different parties but provide identical information. Also see *Financial Market Preparedness: Improvements Made, but More Action Needed to Prepare for Wide-Scale Disasters*, GAO-04-984 (Washington, D.C.: Sept. 27, 2004); *Financial Market Organizations Have Taken Steps to Protect against Electronic Attacks, but Could Take Additional Actions*, GAO-05-679R (Washington, D.C.: June 29, 2005); *Financial Market Preparedness: Significant Progress Has Been Made, but Pandemic Planning and Other Challenges Remain*, GAO-07-399 (Washington, D.C.: Mar. 29, 2007).

of the securities markets—and compared these plans against criteria that regulators have issued that outline the key elements that an organization should include in its pandemic plans and preparations. We also reviewed a randomly selected sample of examinations of broker-dealer firms that clear trades for others. For security reasons, we did not include the names or locations of the seven organizations we reviewed in this report. In addition, we interviewed the relevant securities and banking regulators—including the Securities and Exchange Commission (SEC), the Financial Industry Regulatory Authority (FINRA), the Board of Governors of the Federal Reserve System (Federal Reserve), and the Office of the Comptroller of the Currency. We also reviewed regulatory pandemic guidance, reports, and supporting documents for examinations conducted by these regulators. We conducted this performance audit from June 2008 to October 2009 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. (More information on our scope and methodology is contained in app. I.)

Background

An influenza pandemic can occur when an existing virus mutates into a novel strain that is highly transmissible among humans, leading to outbreaks worldwide. Such strains can be highly pathogenic because there is little or no pre-existing immunity in the population.[2] Some of the issues associated with the preparation for and responses to an influenza pandemic are similar to those for any other type of disaster or hazard. However, a pandemic poses some unique challenges. Unlike incidents that are discretely bounded in space or time (e.g., most natural or man-made disasters), an influenza pandemic is an event likely to come in waves, each lasting weeks, months, or years, and pass through communities of all sizes across the nation and the world. While a pandemic will not directly damage physical infrastructure such as power lines or computer systems, it could threaten critical systems by potentially removing the essential personnel needed to operate them from the workplace for weeks or months. The World Health Organization (WHO) and the U.S. Centers for

[2]Although the current pandemic is caused by a strain of the H1N1 influenza virus, experts remain concerned that other influenza viruses—such as the H2N2, H5N1, and H7N7—also have the potential to cause a pandemic.

Disease Control and Prevention (CDC) have said that in a severe pandemic, the absences of those who are ill, taking care of ill family members, and fearing infection could reach a projected 40 percent during the peak weeks of a community outbreak, with lower rates of absence during the weeks before and after the peak. In addition, an influenza pandemic could result in 200,000 to 2 million deaths in the United States, depending on its severity. Although representing a novel strain of flu, the H1N1 outbreak, first detected in the United States around April 2009, has caused illness ranging from mild to severe. While most people who have been sick have recovered without needing medical treatment, hospitalizations and deaths from infection with this virus have occurred, and recent CDC news bulletins have indicated the second wave of the disease potentially could be more severe, especially for children and other at-risk groups.

As with most disasters, the initial governmental response to a pandemic will be at the state and local level and will aim to decrease people's exposure to the virus. Initial responses may include encouraging and facilitating good hand hygiene, requiring ill individuals to isolate themselves, educating people about conditions that put them at high risk for complications, encouraging early treatment, and encouraging creative solutions to increase the distance between people at school and work. Under conditions of increased severity of illness, government response could escalate to include more aggressive actions such as closing schools, shutting down public transportation, and prohibiting large public gatherings at venues such as sporting events. These measures are intended to create "social distance" between people to prevent large numbers of people coming into direct contact in an attempt to minimize transmission of the disease. Similarly, individual organizations are also advised to increase the distance between people in workplaces. At the federal level, the National Strategy for Pandemic Influenza Implementation Plan calls for the Secretary of HHS to lead the federal medical response to a pandemic, and the Secretary of DHS to lead the overall domestic incident management and federal coordination.[3]

[3]Homeland Security Council, *National Strategy for Pandemic Influenza Implementation Plan* (May 2006).

Various Agencies Have Responsibility for Ensuring That Critical Telecommunications and Financial Sector Infrastructures Are Protected

Protecting the nation's critical infrastructure against natural and manmade catastrophic events, including pandemic, has been a concern of the federal government for over a decade. Several federal policies address the importance of coordination between the government and the private sector in critical infrastructure protection. Homeland Security Presidential Directive 7 (HSPD-7), issued in December 2003, identifies various federal agencies, including DHS, as having responsibility for ensuring that steps are taken to protect specific critical infrastructure sectors of the United States.[4] HSPD-7 makes DHS responsible for, among other things, coordinating national critical infrastructure protection efforts and establishing uniform policies, approaches, guidelines, and methodologies for integrating federal infrastructure protection and risk management activities within and across these sectors.

In addition to other sectors, DHS is the lead federal agency for two critical infrastructure sectors—information technology (IT) and communications—that are important for the Internet.[5] Specifically, the entities within DHS responsible for coordinating national efforts to promote critical infrastructure protection activities for those sectors are the National Cyber Security Division and the Office of the Manager of the National Communications System (NCS), respectively. [6] Although the vast majority of Internet infrastructure is owned and operated by the private sector, federal policy recognizes the need to be prepared for the possibility of debilitating disruptions in cyberspace. With the exception of the Department of Defense and intelligence community networks, DHS is the central coordinator for cyberspace security efforts and has responsibility for developing an integrated public-private plan for Internet recovery.[7] FCC, which was established under the Communications Act of 1934 to regulate interstate and international communications by radio, television,

[4]The White House, *Homeland Security Presidential Directive/HSPD 7: Critical Infrastructure Identification, Prioritization, and Protection* (December 2003). While HSPD-7 identifies 17 critical infrastructure sectors, the directive allows for DHS to identify gaps in existing infrastructure sectors as well as establish new sectors to fill these gaps. Under this authority, DHS established an 18th sector—critical manufacturing—in March 2008.

[5]DHS also is the lead federal agency for nine other critical infrastructure sectors.

[6]Both of these offices are within the Office of Cybersecurity and Communications, which is a part of the National Protection and Programs Directorate.

[7]The White House, *National Strategy to Secure Cyberspace* (Washington, D.C., February 2003).

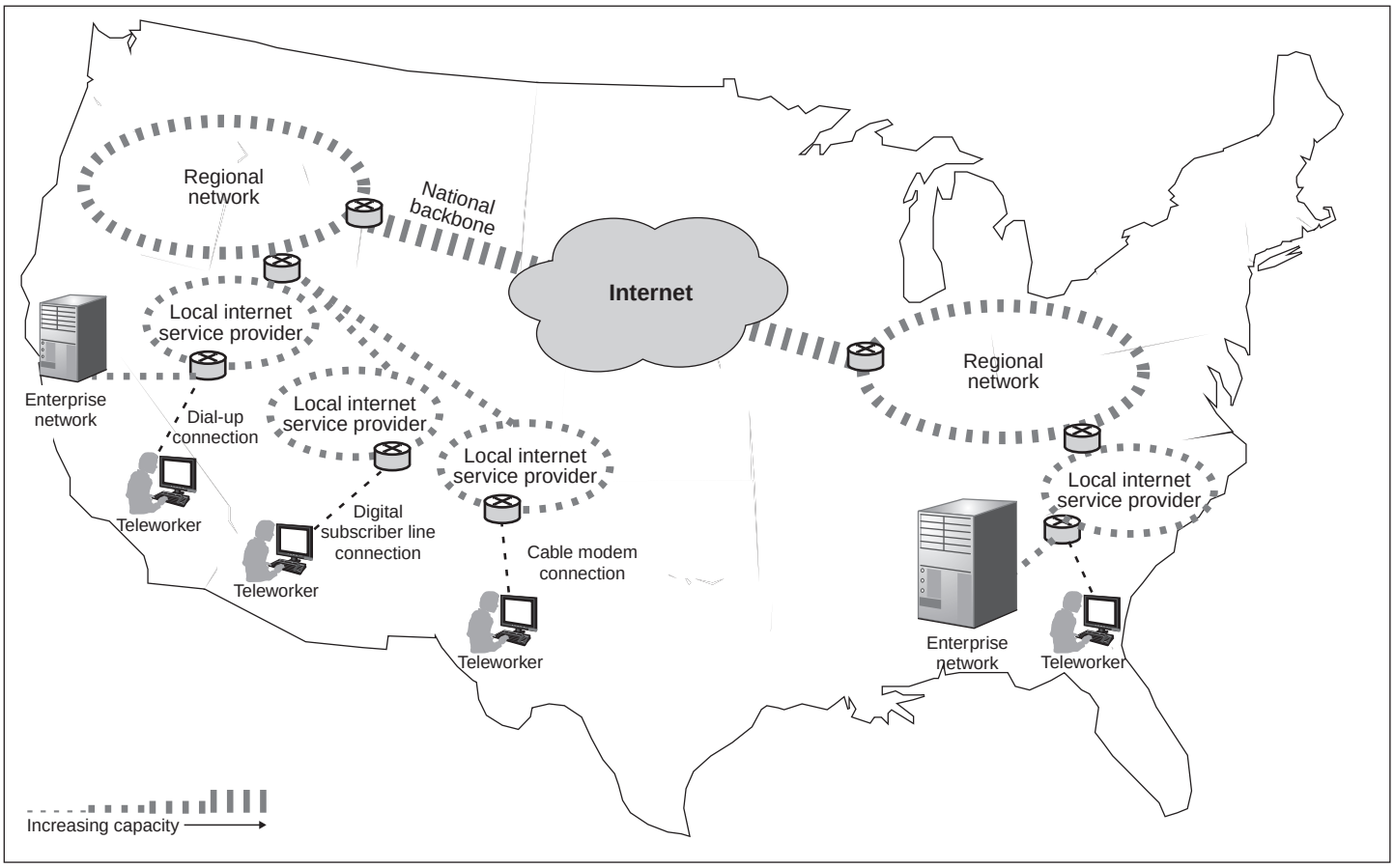
wire, satellite, and cable—also oversees the telecommunications infrastructure on which the Internet depends.[8] Because the functioning of the financial markets is important for our nation's economy, the financial sector is one of the infrastructure sectors that has been designated as critical. Finally, under HSPD-7, the Department of the Treasury (Treasury) is responsible for infrastructure protection activities specifically within the banking and finance sector.

Private Companies Provide the Networks That Comprise the Internet

The public Internet infrastructure is owned and operated primarily by private companies such as telecommunications companies, cable companies, and other Internet service providers. It is a network of many networks used around the world to communicate and share computing resources, engage in commerce, do research, and provide entertainment. As shown in figure 1, the various networks that make up the Internet include the national backbone and regional networks, as well as the residential Internet access networks and the networks run by individual businesses, or "enterprise" networks. The national backbone providers transmit data over long distances using high-speed fiber-optic lines. Because these providers do not service all locations worldwide, regional network providers provide regional service to supplement the long-haul traffic. When a user wants to access a Web site or send an e-mail to someone who is connected to the Internet through a different service provider, the data must be transferred between networks. Data travels from a user's home computer to the Internet through various means, including coaxial cable, digital subscriber line (DSL), satellite, fiber, or wirelessly to a provider's facility where it is aggregated with other users' traffic. Data cross between networks at Internet exchange points, which can be either hub points where multiple networks exchange data or private interconnection points. At these exchange points computer systems called routers determine the optimal path for the data to reach their destination. The data then continue through the national and regional networks and exchange points, as necessary, to reach the recipient's Internet service provider and the recipient.

[8] 47 U.S.C. § 151 et. seq.

Figure 1: Overview of the Internet



Sources: GAO.

A functioning Internet will be important during a pandemic because it could be one important way that governments and private entities share necessary information with the public. Using the Internet to allow people to communicate effectively without coming together physically would assist in creating "social distance" to reduce the potential for illness to further spread. In addition, many organizations, including DHS, have been advocating that businesses and other enterprises consider increased use of telework by their workforce as a way to continue operations while maintaining physical separation from other workers during a pandemic. Doing so would typically involve employees working from home and accessing their business's networks over an Internet connection. Some entities have also advocated the use of the Internet as a means for

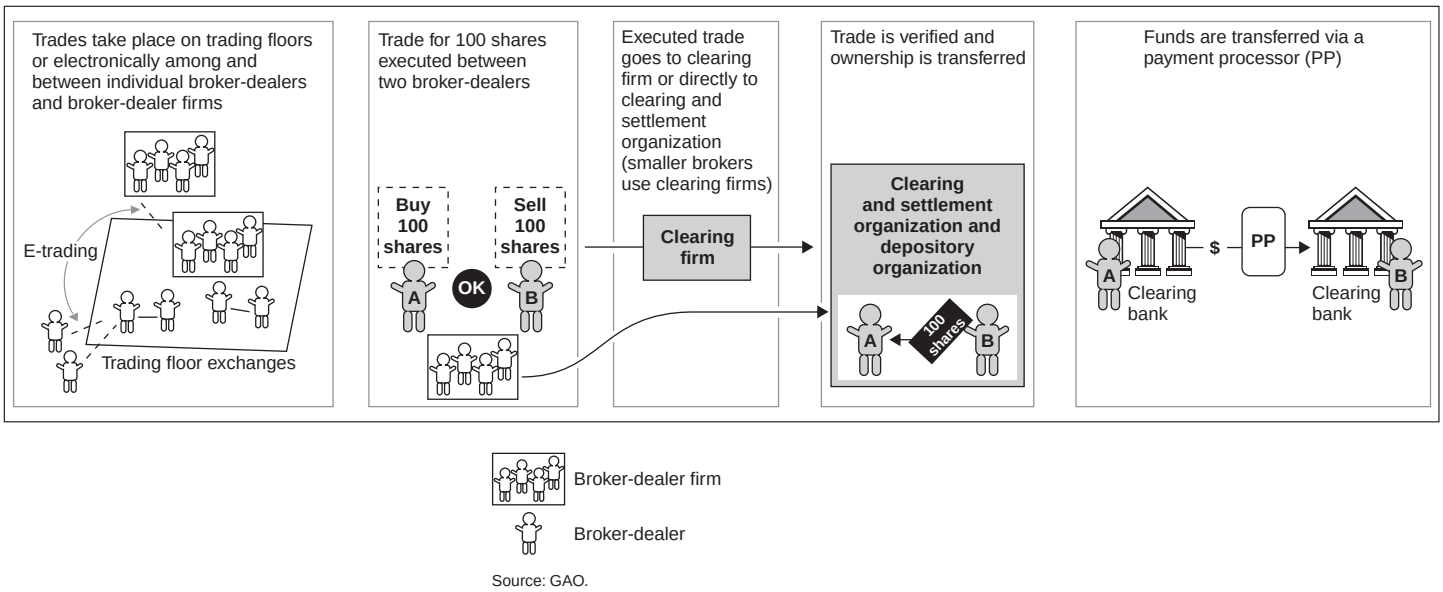
reducing the social isolation that could arise when people are asked to avoid contact with others.

Functioning Securities Markets Require Participation by Various Types of Organizations

For the U.S. securities markets to function, ensuring that companies can raise capital to carry on commerce and investors can obtain returns on their savings for spending on necessities or for retirement security, various organizations must be able to operate. Individual investors and institutions such as mutual funds send their orders to buy and sell stocks and options to broker-dealers that, in turn, route these orders to be executed at one of the many exchanges or electronic trading venues in the United States and abroad. After a securities trade is executed, it undergoes clearance and settlement to verify the accuracy of the transaction. Ownership of the securities is then transferred from the seller to the buyer, and the necessary payment between the two parties is exchanged. Separate organizations complete the clearance and settlement process for stocks and for options. In general, a clearing organization collects and compares trade information to ensure the accuracy of the trade and calculates the amounts that are to be exchanged between parties. A depository organization then transfers ownership and maintains the records of securities held by broker-dealers and investors. To facilitate these interactions, the large broker-dealers have accounts directly with the clearing organizations, while smaller and independent broker-dealers act as introducing firms by sending their customers' orders to an intermediary broker-dealer, known as a clearing firm, that accepts and processes the trades and clears and settles these trades with the central clearing organization. The clearing firm's systems also maintain the records of the cash and securities holdings of the introducing broker-dealers, and their investor customers.

The monies transferred as part of securities transactions are handled by the banks that maintain accounts for broker-dealers and accept and make payments for these firms' securities activities. Payment processing systems operated by the Federal Reserve or private firms process the payments that are exchanged between the clearing banks used by the clearing organizations, broker-dealers, and their customers. Virtually all of the information processed is transferred electronically between parties; clearance and settlement and payment transactions take place over proprietary networks that do not traverse the public Internet infrastructure. Figure 2 illustrates how these various organizations participate in a trade.

Figure 2: Role of Various Securities Market Participants in a Typical Securities Trade



Source: GAO.

Although thousands of entities are active in the U.S. securities markets, certain key organizations are more critical to the ability of the markets to function, usually because they offer unique products or perform vital services. For example, markets cannot function without the activities performed by clearing organizations and in some cases, only one clearing organization exists for particular products. In addition, other market participants are critical to overall market functioning because they consolidate and distribute price quotations or information on executed trades. The inability of any one broker-dealer firm to continue operations during an event would not likely affect the markets as a whole, but a small number of large broker-dealers generally account for sizeable portions of the daily trading volume on many exchanges. If several of these large firms were unable or unwilling to operate, the markets might not have sufficient trading volume to function in an orderly or fair way. U.S. securities markets have evolved in the last decade, with trading occurring at a larger number of venues, including existing exchanges, electronic markets, and alternative trading networks operated by broker-dealers or others. As a result, the criticality of some participants to the overall functioning of the

markets likely has changed since we began reviewing these issues in 2001, but all continue to play significant roles in U.S. markets.[9]

Several Organizations Oversee the Various Securities Market Participants

Various regulators oversee securities market participants:

- SEC regulates the stock and options exchanges and the clearing organizations for those products. In addition, SEC issues rules and oversees the broker-dealers that trade on those markets and other participants, such as mutual funds, which are active investors.
- Self-regulatory organizations also oversee broker-dealers directly and are responsible for ensuring that their members comply with the securities laws and these organizations' own rules. FINRA is the primary self-regulatory organization for securities firms conducting business in the United States.[10] As part of its responsibilities, this regulator conducts examinations of its members to ensure compliance with its rules and federal securities laws.
- The clearing banks that maintain accounts on behalf of securities market participants are overseen primarily by two different regulators. The Federal Reserve oversees bank holding companies and state-chartered banks that are members of the Federal Reserve System. The Office of the Comptroller of the Currency examines nationally chartered banks.

[9]Although some of the seven organizations that we have considered critical to the markets' overall ability to function may have lessened, each continues to play an important role. As a result, we continue to use this group of organizations during our assessment to provide continuity to this report and to those that we issued previously.

[10]Since the passage of the Securities Exchange Act in 1934, 15 U.S.C. § 78a et seq., the stock and options exchanges have acted as self-regulatory organizations by ensuring that the broker-dealers that traded on their markets complied with the rules of their market and with the securities laws in general. SEC also is responsible for ensuring that the requirements of these laws are followed.

Securities Market Organizations and Regulators Have Been Addressing Threats to Critical Market Operations since 2001

As we reported in a series of reports issued since the September 11, 2001 terrorist attacks, securities market organizations have made significant progress in addressing various threats with the potential to disrupt their operations. [11] As we reported in 2007, the group of organizations that we considered critical to overall operations of the securities markets—including exchanges, clearing organizations, and payment processors—have acted to significantly reduce the likelihood of physical disasters disrupting the functioning of U.S. securities markets. For example, all these organizations had developed the capability to perform their critical functions at alternate sites geographically dispersed from their primary sites. They all also had improved their physical and information security measures. The broker-dealers and clearing services banks that account for significant trading volumes had also taken steps to increase the distances between their sites for primary and backup operations for clearance and settlement activities and established dispersed backup trading locations.

Market participants have also worked with financial regulators and other organizations on other efforts to improve the overall resiliency of the financial sector; these include periodically conducting industry-wide connectivity testing from backup locations. Coordinated by the Securities Industry and Financial Markets Association and other groups, these tests verify the ability of market participants to operate through an emergency using backup sites, recovery facilities, and backup communications capabilities across the industry; and to provide participants with an opportunity to exercise and check the ability of their backup sites to successfully transmit and receive communications between the backup sites of other market participants. In the 2008 test, more than 250 organizations, including broker-dealers, markets, service bureaus, and industry utilities participated, with test participants representing more than 85 percent of normal market volume. Overall, almost 98 percent of test connections among participants were successful. Financial market organizations have also taken steps to be better prepared for physical or information security attacks. For example, DHS's Office of Infrastructure Protection assisted some financial market organizations by conducting assessments of the physical security measures these organizations were taking to prevent damage by physical attacks, including reviewing these organizations' facilities and their physical security measures such as surveillance, perimeter, and intrusion technologies. Officials from Treasury and representatives of selected financial markets also

[11] GAO-03-251, GAO-03-414, GAO-04-984, GAO-05-679R, and GAO-07-399.

participated in exercises conducted by DHS that involved tabletop events that were intended to create lifelike scenarios of disasters or cyber attacks. These exercises were to help participants better understand the effect of cross-sector dependency (or interdependencies) during such events.

To assist in infrastructure protection issues, representatives from a broad range of financial regulatory agencies formed the Financial and Banking Information Infrastructure Committee (FBIIC). This group meets regularly to communicate information and coordinate efforts among the financial regulators and enhance the resiliency of the financial sector.[12] In addition, representatives of the financial trade associations and other entities share information relating to infrastructure protection among financial market participants through the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC).[13] Formed in 2002, FSSCC acts as the private sector council that assists Treasury in addressing critical infrastructure protection issues within the banking and finance sector. FSSCC works to help reinforce the financial services sector's resilience against terrorist attacks and other threats to the nation's financial infrastructure. FSSCC has published reports summarizing best practices and lessons learned for issues of common concern to the industry at large. Members of FSSCC also meet periodically with the financial regulators to share information about common concerns and challenges. Financial market organizations also have received consolidated information through other sources. For example, the

[12]FBIIC members include Commodity Futures Trading Commission, Conference of State Bank Supervisors, Farm Credit Administration, Federal Deposit Insurance Corporation, Federal Housing Finance Board, Federal Reserve Bank of New York, Federal Reserve, 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, SEC, Securities Investor Protection Corporation, and Treasury.

[13]Under the framework established by DHS's National Infrastructure Implementation Plan, each of the critical infrastructure sectors has both a government council and a private sector council to address sector-specific planning and coordination. FBIIC and FSSCC serve the banking and financial sector in that capacity.

Financial Services Information Sharing and Analysis Center (FS/ISAC) consolidates threat information for the sector.[14]

The financial sector has also taken steps to ensure that key officials from financial regulators and financial market organizations will be able to communicate during disasters. Under the Government Emergency Telecommunications Service (GETS) Program, participating staff receive a card that provides them with a code that can be dialed to increase the priority of telephone calls they place during crises. To better ensure that critical communication among financial market participants occurs, FBIIC issued an interim policy on the GETS Card Program in July 2002 that outlines how staff from financial institutions can obtain such cards. To qualify for GETS sponsorship, the FBIIC policy states that organizations must perform functions critical to the operation of key financial markets. This priority currently is only available for voice calls and not for data communications over the Internet. Another FBIIC telecommunications effort involves the FCC's Telecommunications Service Priority (TSP) Program, which is used to identify and prioritize telecommunication services that support national security or emergency preparedness missions. Under TSP, private-sector organizations, through the sponsorship of a selected group of federal agencies, including SEC and the Federal Reserve, can have some of their key telecommunications circuits added to an inventory maintained by NCS that will provide increased priority for restoration of these key circuits in the event of a disruption.

[14]FS/ISAC was established in response to Presidential Directive 63 (1998). That directive—which has since been superseded by 2003 Homeland Security Presidential Directive 7—mandated that the public and private sectors share information about physical and cyber security threats and vulnerabilities to help protect the U.S. critical infrastructure. The White House, *Presidential Decision Directive/NSC-63: Critical Infrastructure Protection* (May 1998).

Internet Congestion During a Severe Pandemic That Hampers Teleworkers Is Anticipated, but Responsible Government Agencies Have Not Developed Plans to Address Such Congestion and May Lack Clear Authority to Act

Increased use of the Internet by students, teleworkers, and others during a severe pandemic is expected to create congestion in Internet access networks that serve metropolitan and other residential neighborhoods. For example, localities may choose to close schools and these students, confined at home, will likely look to the Internet for entertainment, including downloading or "streaming" videos, playing online games, and engaging in potential activities that may consume large amounts of network capacity (bandwidth). Additionally, people who are ill or are caring for sick family members will be at home and could add to Internet traffic by accessing online sites for health, news, and other information. This increased and sustained recreational or other use by the general public during a pandemic outbreak will likely lead to a significant increase in traffic on residential networks. If theaters, sporting events, or other public gatherings are curtailed, use of the Internet for entertainment and information is likely to increase even more. Furthermore, the government has recommended teleworking as an option for businesses to keep operations running during a pandemic. Thus, many workers will be working from home, competing with recreational and other users for bandwidth.

According to a DHS study and Internet providers, this additional pandemic-related traffic is likely to exceed the capacity of Internet providers' network infrastructure in metropolitan residential Internet access networks.[15] Residential Internet users typically connect their computers to their Internet service providers' network through a modem or similar Internet access device. These Internet access devices route home users' traffic to a network device that aggregates it with that of other users before forwarding it to the other parts of the provider's network and its ultimate destination on the Internet. As shown in figure 3, the traffic aggregating device differs depending on the technology used for Internet access—DSL, a cable network, or other means. But all these technologies use network architectures that basically aggregate the traffic of multiple users on a single device that then routes it to other parts of the providers' networks. For example, within a DSL network architecture, the user's traffic travels on a dedicated pair of copper wires from a home computer to the provider's location—usually known as a central office—which houses a device called the digital subscriber line access multiplexer

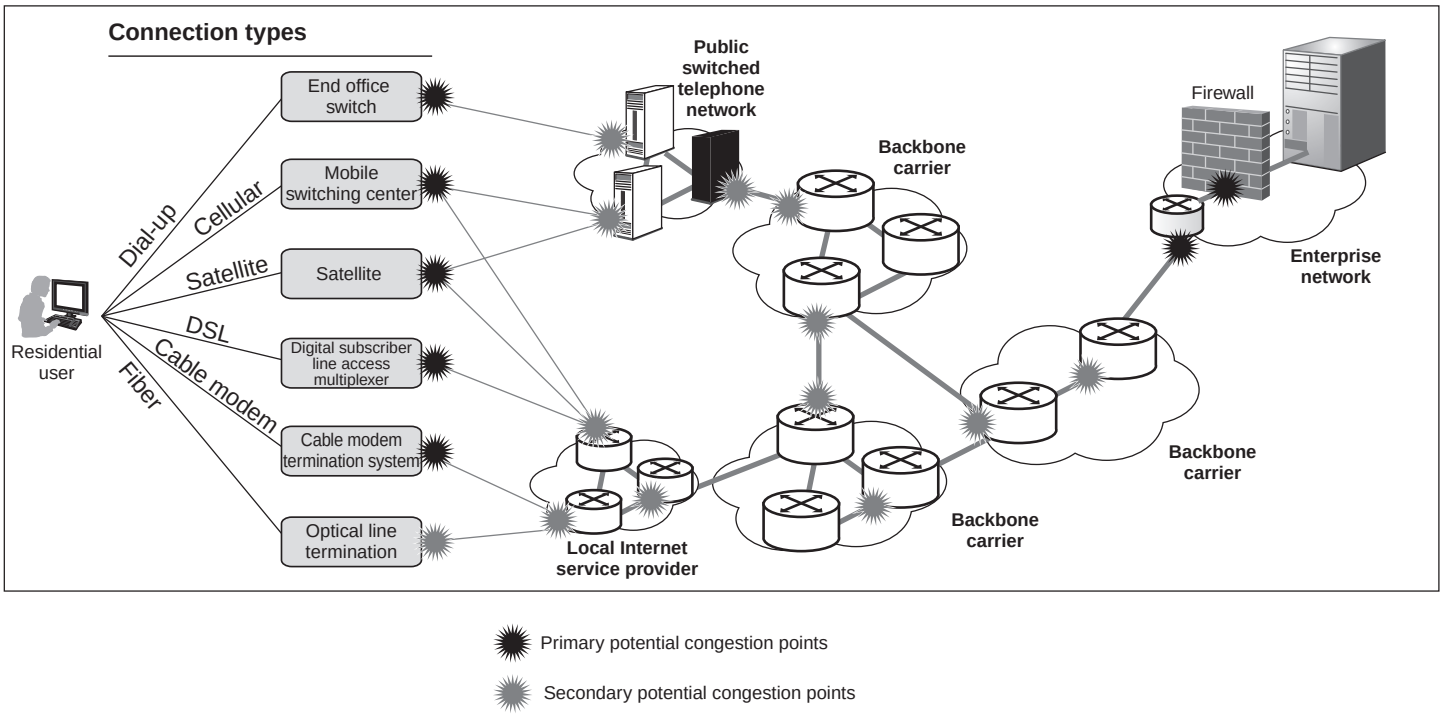
[15]According to one provider, this additional traffic in residential neighborhoods may not result in an increase in Internet traffic overall because it may be traffic that would have otherwise come from businesses in other parts of the Internet access networks, but during a pandemic would originate in the residential access portions of the networks instead.

(DSLAM). The DSLAM aggregates this traffic and that of other users of this provider from individual residential neighborhoods before sending it on to regional networks and eventually to the national Internet backbone.[16] Traffic from home users who connect to the Internet through a cable provider moves from the home computer over coaxial cables and fiber optic cables then ultimately to a network device known as a cable modem termination system (CMTS). The CMTS also aggregates this traffic with that of other users from other individual residential neighborhoods and sends it to the regional networks and the national Internet backbone.[17] During a pandemic, congestion is most likely to occur in the traffic to or from the aggregation devices that serve residential neighborhoods, interfering with teleworkers' and others' ability to use the Internet.

[16]A DSLAM is a network device, usually at a telephone company central office, that receives signals from multiple customer DSL connections and puts the signals on a high-speed backbone line by channeling many inputs onto one output.

[17]According to one provider, in a cable environment both the incoming and outgoing traffic share a fixed amount of bandwidth as it moves over coaxial cables between the modems and a node onto fiber. Eventually, traffic aggregates at a port on a CMTS. A CMTS is a device located in a cable operator's local network that acts as the gateway to the Internet for cable modems in a particular geographic area.

Figure 3: Potential Points of Congestion



Source: GAO (based on DHS information).

Congestion affecting home users is likely to occur because the parts of providers' DSL, cable, satellite, and other types of networks that provide access to the Internet from residential neighborhoods are not designed to carry all the potential traffic that users could generate in a particular neighborhood or that all connect to a particular aggregating device for efficiency and cost reasons. Providers do not build networks to handle 100 percent of the total traffic that could be generated because users are neither active on the network all at the same time, nor are they sending maximum traffic at all times. Instead, providers use statistical models based upon past users' patterns and projected growth to estimate the likely peak load of traffic that could occur and then design and build networks based on the results of the statistical model to accommodate at least this level. According to one provider, this engineering method serves to optimize available capacity for all users. For example, under a cable architecture, 200 to 500 individual cable modems may be connected to a provider's CMTS, depending on average usage in an area. Although each of these individual modems may be capable of receiving up to 7 or 8 megabits per second (Mbps) of incoming information, the CMTS can transmit a

maximum of only about 38 Mbps.[18] Providers' staff told us that building the residential parts of networks to be capable of handling 100 percent of the traffic that all users could potentially generate would be prohibitively expensive.

A 2007 DHS study that was conducted in cooperation with various government, communication sector, and financial sector entities used modeling of residential and other network configurations to confirm that the increased traffic generated in neighborhoods during a severe pandemic is likely to exceed the capacity of the providers' aggregation devices in metropolitan residential neighborhoods.[19] The study examined the technical feasibility of the pandemic telecommuting strategy advocated by the government. The study also focused on identifying action plans to better prepare the nation for telecommuting during an influenza pandemic. As part of the study, a model was developed using data and assumptions from a large U.S. metropolitan area to represent a typical Internet provider's network configuration, including devices and network capacities. For cost reasons, the study used DSL network architecture for the purposes of the congestion modeling, but the preparers acknowledged that other means of accessing the Internet had similar architectures and thus the impact of a pandemic would be similar. The contractors that prepared the study simulated Internet traffic in amounts that corresponded to the level of Internet use in a residential neighborhood under three scenarios of pandemic severity—20, 40, and 90 percent absenteeism from the workplace. The study's model predicted that at the 40 percent absenteeism level—the level that health organizations have indicated is likely under a relatively serious pandemic—the highest point of congestion across the entire Internet infrastructure could occur within residential Internet access networks. Specifically, at the 40 percent absenteeism level, the study predicted that most users within residential neighborhoods would likely experience congestion when attempting to use the Internet. Based on our assessment of the study, we concluded that the methodology applied and the likely congestion points identified were reasonable. Furthermore, communication sector representatives we

[18]Network performance is measured in bits per second or bps. One megabit per second equals 1 million bps. Due to the historically incoming-focused nature of Internet usage, according to one provider, cable networks typically provide one 6-megahertz (MHZ) channel with a capacity of 38.2 Mbps in the incoming direction.

[19]Department of Homeland Security, *Pandemic Influenza Impact on Communications Networks Study* (Washington, D.C., December 2007).

interviewed confirmed the likelihood of Internet congestion between a user's home and the point at which that traffic combines with other users at the providers' aggregation devices. Although this study assessed the impact on a large city, the severity of congestion could vary across neighborhoods or nationally depending on the capacities of residential neighborhood Internet access networks, with cities or areas with larger populations and higher incomes generally having large broadband capacities and less-populated rural or poorer areas possibly having less broadband capacity. However, the study used typical telecommunications network configurations for a large U.S. city and found that congestion was likely. As a result, we believe that its findings mean that most other locations in the United States could experience similar problems.

Although predicting that the most severe congestion would occur within residential access networks, the study overseen by DHS also noted that pandemic-related congestion was possible in other parts of the networks that comprise the Internet. For example, users could experience congestion at the point at which traffic is transferred between service providers because of potential differences in transmission capacity. Additionally, teleworkers connecting to their companies' networks (the "enterprise" networks) could overload various components of these networks, such as the devices that provide security—firewalls—or servers that provide access to various applications because some businesses' networks may not have scaled these devices to accommodate the anticipated increase in telecommuting traffic during a pandemic. The steps being taken by financial organizations to ensure their enterprise networks are prepared for pandemic levels of use are discussed later in this report.

Providers' Options for Reducing Internet Congestion Are Limited and Could Require Government Action

Providers' options for addressing expected pandemic-related Internet congestion include providing extra capacity, using network management controls, installing direct lines to organizations, temporarily reducing the maximum transmission rate, and shutting down some Internet sites. Each of these methods is limited either by technical difficulties or questions of authority. In the normal course of business, providers attempt to address congestion in particular neighborhoods by building out additional infrastructure—for example, by adding new or expanding lines and cables. Internet provider staff told us that providers determine how much to invest in expanding network infrastructure based on business expectations. If they determine that a demand for increased capacity exists that can profitably be met, they may choose to invest to increase network capacity in large increments using a variety of methods such as replacing old equipment and increasing the number of devices serving

particular neighborhoods. Providers will not attempt to increase network capacity to meet the increased demand resulting from a pandemic, as no one knows when a pandemic outbreak is likely to occur or which neighborhoods would experience congestion. Staff at Internet providers whom we interviewed said they monitor capacity usage constantly and try to run their networks between 40 and 80 percent capacity at peak hours. They added that in the normal course of business, their companies begin the process to expand capacity when a certain utilization threshold is reached, generally 70 to 80 percent of full capacity over a sustained period of time at peak hours.

However, during a pandemic, providers are not likely to be able to address congestion by physically expanding capacity in residential neighborhoods for several reasons. First, building out infrastructure can be very costly and takes time to complete. For example, one provider we spoke with said that it had spent billions of dollars building out infrastructure across the nation over time, and adding capacity to large areas quickly is likely not possible. Second, another provider told us that increasing network capacity requires the physical presence of technicians and advance planning, including preordering the necessary equipment from suppliers or manufacturers. The process can take anywhere from 6 to 8 weeks from the time the order is placed to actual installation. According to this provider, a major constraint to increasing capacity is the number of technicians the firm has available to install the equipment. In addition to the cost and time associated with expanding capacity, during a pandemic outbreak providers may also experience high absenteeism due to staff illnesses, and thus might not have enough staff to upgrade network capacities. Providers said they would, out of necessity, refrain from provisioning new residential services if their staff were reduced significantly during a pandemic. Instead, they would focus on ensuring services for the federal government priority communication programs and performing network management techniques to re-route traffic around congested areas in regional networks or the national backbone.[20] However, these activities would likely not relieve congestion in the residential Internet access networks.

[20]These programs include GETS, TSP, and the Wireless Priority Service, which are intended to ensure that (1) emergency response personnel are able to communicate with the federal, state, and local leadership for decisions involving emergency response and (2) telecommunications services are restored or added on a priority basis during disasters.

Providing critical employees direct connections that bypass residential congestion may be another option for facilitating telework during a pandemic, but this option can be cost prohibitive to employers and is not widely used. Specifically, some providers offer network solutions such as private lines to businesses and governments. Private line services allow businesses to run their corporate networks and applications separately from public Internet traffic and could provide a point-to-point dedicated path between teleworkers' homes and offices, bypassing the residential neighborhood congestion points. However, according to provider staff we spoke with, installing private lines in a residence requires advance planning and is expensive. One provider noted that a direct connection is not a solution that can be invoked when the pandemic strikes.

Technically Feasible Options Would Likely Require a Government Directive

In the current network environment, providers' capability to address pandemic-related Internet congestion by prioritizing certain users' traffic, including that of financial sector teleworkers, is limited. Specifically, provider systems are not designed to identify and provide priority to individual users when traffic is routed over the Internet and multiple networks are used for the connection.[21] Furthermore, Internet providers' networks also are not currently designed to identify particular types of customers connected to the Internet. For example, the networks cannot distinguish between critical employees teleworking and recreational users.

Providers identified one technically feasible alternative that has the potential to reduce Internet congestion during a pandemic, but raised concerns that it could violate customer service agreements and thus would require a directive from the government to implement. Although providers cannot identify users at the computer level to manage traffic from that point, two providers stated that if the residential Internet access network in a particular neighborhood was experiencing congestion, a provider could attempt to reduce congestion by reducing the amount of traffic that each user could send to and receive from his or her network. Such a reduction would require adjusting the configuration file within each customer's modem to temporarily reduce the maximum transmission speed that that modem was capable of performing—for example, by reducing its incoming capability from 7 Mbps to 1 Mbps. However,

[21]According to one provider we spoke with, they have a specialized congestion management system that is capable of temporarily deprioritizing some users' traffic during times of congestion. This practice is based on identifying users that are contributing significantly to congestion. However, this capability is not technically feasible to identify and prioritize traffic based on a list of specific users.

according to providers we spoke with, such reductions could violate the agreed-upon levels of services for which customers have paid. Therefore, under current agreements, two providers indicated they would need a directive from the government to take such actions.

Shutting down specific Internet sites would also reduce congestion, although many we spoke with expressed concerns about the feasibility of such an approach. Overall Internet congestion could be reduced if Web sites that accounted for significant amounts of traffic—such as those with video streaming—were shut down during a pandemic. According to one recently issued study, the number of adults who watch videos on video-sharing sites has nearly doubled since 2006, far outpacing the growth of many other Internet activities.[22] However, most providers' staff told us that blocking users from accessing such sites, while technically possible, would be very difficult and, in their view, would not address the congestion problem and would require a directive from the government.[23] One provider indicated that such blocking would be difficult because determining which sites should be blocked would be a very subjective process. Additionally, this provider noted that technologically savvy site operators could change their Internet protocol addresses, allowing users to access the site regardless. Another provider told us that some of these large bandwidth sites stream critical news information. Furthermore, some state, local, and federal government offices and agencies, including DHS, currently use or have plans to increase their use of social media Web sites and to use video streaming as a means to communicate with the public. Shutting down such sites without affecting pertinent information would be a challenge for providers and could create more Internet congestion as users would repeatedly try to access these sites. According to one provider, two added complications are the potential liability resulting from lawsuits filed by businesses that lose revenue when their sites are shutdown or restricted and potential claims of anticompetitive practices, denial of free speech, or both. Some providers said that the operators of specific Internet sites could shut down their respective sites with less disruption and more effectively than Internet providers, and suggested that a better course of action would be for the government to work directly with the site operators.

[22]Pew Research Center, *The Audience for Online Video-Sharing Sites Shoots Up* (July 2009).

[23]A fuller discussion related to the legal authorities surrounding the Internet follows in the next section of this report.

Additional Capabilities to Prioritize Traffic or Expand Capacities May Be Available in the Future

Providers could help reduce the potential for a pandemic to cause Internet congestion by ongoing expansions of their networks' capacities. Some providers are upgrading their networks by moving to higher capacity modems or fiber-to-the-home systems. For example, some cable providers are introducing a network specification that will increase the download capacity of residential networks from the 38 Mbps to about 152 to 155 Mbps.[24] In addition to cable network upgrades, at least one telecommunications provider is offering fiber-to-the home, which is a broadband service operating over a fiber-optic communications network. Specifically, fiber-to-the-home Internet service is designed to provide Internet access with connection speeds ranging from 10 Mbps to 50 Mbps.

Although not generally feasible in the current environment, the ability to prioritize individual user's traffic is envisioned to be technically possible in future upgrades of the infrastructure of the Internet and telecommunications networks, but such capabilities are estimated to be years away. As we recently reported, DHS is working with international standards bodies to help develop standards that could allow greater flexibility to prioritize data communications in the future;[25] this effort is a part of what is referred to as the Next Generation Networks.[26] However, these capabilities are not expected to be ready for several years due to the complexity of the systems and the need to develop standards that work across varying providers' infrastructures, including internationally. In addition, we reported DHS had difficulty getting its full budgets approved, which may have contributed to the delay in developing standards. As a result, the expanded features of this newer network architecture are not expected to be a viable solution for addressing pandemic-related Internet congestion in the near future.

[24]This specification is known as the data over cable service interface specification or DOCSIS. Currently, cable providers are generally using DOCSIS 1.0, 1.1, and 2.0. Cable providers are deploying the upgraded specification, which is known as DOCSIS 3.0. This standard, which includes incoming and outgoing channel bonding permits dramatic capacity increase—four channels, each capable of 38 Mbps downloading capacity.

[25]GAO, *Emergency Communications: National Communications System Provides Programs for Priority Calling, but Planning for New Initiatives and Performance Measurement Could Be Strengthened*, GAO-09-822 (Washington, D.C.: Aug. 28, 2009).

[26]According to the President's National Security Telecommunications Advisory Committee *Next Generation Networks Task Force Report* (March 2006), the Next Generation Networks represent the set of converged networks expected to arise that will transparently carry many types of data and communications and allow delivery of services and applications that are not coupled to the underlying network.

DHS Has Done Some Pandemic Planning but Has Not Taken Actions Needed to Effectively Address Potential Pandemic-related Internet Congestion

Although responsible for coordinating protection of the communications-critical infrastructure sector, which includes the networks that comprise the Internet, DHS has not yet developed a strategy to address pandemic-related Internet congestion, coordinated with federal partners, determined if sufficient authority exists to take necessary actions, or assessed the need for a public communications campaign to minimize congestion that is expected to occur during a pandemic. Under HSPD-7 and the National Strategy to Secure Cyberspace, DHS is the lead agency for coordinating the protection of critical assets in the communications sector from attacks.[27] Also under these authorities, DHS is responsible for facilitating a public-private response to the recovery from major Internet disruption.[28] In addition to being a focal point to the cyber-critical infrastructure protection effort, DHS has been designated as one of two federal agencies responsible for coordinating the United States' pandemic response. As specified in the *Implementation Plan for the National Strategy for Pandemic Influenza*, DHS is to coordinate the nation's response in conjunction with HHS.

DHS has undertaken several pandemic planning activities. As discussed earlier in this report, DHS and representatives from the government, communications sector, and financial sector conducted a study to assess specifically the technical feasibility of the pandemic telecommuting strategy and identify ways for the nation to better prepare to support the strategy. In coordination with interagency partners and the critical infrastructure sector coordinating councils, DHS has completed individual sector-specific pandemic guidelines and provided Webinars to sector partners on their respective plans. These guidelines are intended to assist the sectors and businesses with the sectors' plan for a severe influenza pandemic, and include some consideration of potential Internet congestion. For example, the guidelines for the information technology

[27]The White House, *National Strategy to Secure Cyberspace* (Washington, D.C., February 2003).

[28]We previously reported that DHS had initiated efforts to refine high-level disaster recovery plans but the components of these plans that pertain to the Internet were not complete. Additionally, while DHS had undertaken several initiatives to improve Internet recovery planning, much remained to be done. Specifically, some initiatives lacked clear timelines, lessons learned were not consistently being incorporated in recovery plans, and the relationships between the various initiatives were not clear. We recommended that DHS take various actions to improve these plans and obtain input from Internet providers. DHS concurred with the recommendation. GAO, *Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan*, GAO-06-672 (Washington, D.C.: June 16, 2006).

and communications sectors recommend that entities in these sectors consider advising employees to limit household use of streaming video or other bandwidth-intensive Internet activities. The guidelines also recommend consideration of obtaining multiple means of accessing the Internet. The guidelines have been provided to the sector coordinating councils via a secure DHS information portal, as well as to the members of the National Governor's Association. DHS officials told us that some of the sectors have made the guidelines available to the public. More recently, DHS completed the *DHS 2009-H1N1 Implementation Plan*, which provides planning guidance for DHS and identifies specific roles and responsibilities for the DHS components such as the Office of Policy or the Transportation Security Administration. According to DHS officials, the plan also directs all DHS components to develop plans that address key preparation and response actions, performance of mission essential functions, workforce protection, continuity of operations, and communications with key stakeholders during the H1N1 influenza pandemic.

However, while these planning activities are designed to help government and private sector partners prepare for a pandemic, they are limited in addressing the anticipated Internet congestion. Although serving as the coordinating agency for Internet recovery and pandemic response, DHS staff told us that their agency does not have a strategy to address Internet congestion. According to DHS staff, their agency has not begun developing such a strategy because since the September 11 terrorist attacks, they have had other crises such as Hurricane Katrina to address. A senior official at a financial markets regulator told us that leadership by the government had been lacking in addressing this potential risk to the financial sector. Without action by DHS to address this potential congestion, employees in critical sectors of the nation's economy, including those in financial services, might not be able to effectively telework or otherwise communicate or transmit data over the Internet.

In addition, although various federal and private sector organizations would likely be required to coordinate an effective Internet congestion response strategy, DHS has neither reached out nor coordinated with other partners, such as other federal or state agencies with telecommunications oversight authorities, to prepare such a strategy. As we previously reported, the experience of Hurricane Katrina showed the need to improve leadership at all levels of government in order to better

respond to a catastrophic disaster.[29] As part of this, the legal authorities, roles and responsibilities, and lines of authority at all levels of government must be clearly defined, effectively communicated, and well understood in order to facilitate rapid and effective decision making. In order to respond effectively to pandemic-related Internet congestion, DHS will need to effectively plan and work with other parts of the federal government and possibly state and local governments and the private sector in its efforts. Other organizations that could be relevant include FCC, which, as previously noted, is charged with regulating interstate and international communications by radio, television, wire, satellite, and cable. DHS staff representing the Office of Policy acknowledged that such coordination would be necessary to address Internet congestion effectively and ensure that the various parts of the federal government are not conducting conflicting activities. For example, the staff told us the Department of Education was hoping to have schools use the Internet during a pandemic to allow students to access remote learning courses if schools were closed. The staff acknowledged that, as a result, DHS would have to coordinate with the other relevant agencies to ensure that their various actions are appropriately taken into account in developing a congestion plan. According to DHS staff, DHS has engaged in dialogues with other agencies about pandemic-related issues on a regular basis. Agency staff once again cited time constraints and the need to focus on other crises as reasons for not having discussed the development of a coordinated strategy for addressing Internet congestion. However, unless DHS starts coordinating with other federal, state, and even private sector parties on possible Internet congestion solutions, there may not be sufficient time to develop a coordinated strategy to address a rapidly emerging severe pandemic.

Further, although an effective congestion response strategy could require directing the private sector entities that operate the Internet's infrastructure today to take actions that could negatively affect users, DHS has not determined whether it or other agencies have the necessary authorities to require providers to take such actions. We previously reported that the authorities of federal government agencies regarding the Internet were unclear.[30] Given the importance of the Internet

[29]GAO, *Catastrophic Disasters: Enhanced Leadership, Capabilities, and Controls Will Improve the Effectiveness of the Nation's Preparedness, Response, and Recovery System*, GAO-06-618 (Washington, D.C.: Sept. 6, 2006).

[30]GAO-06-672.

infrastructure to our nation's communications and commerce, we suggested that Congress consider clarifying the legal framework guiding Internet recovery. Although DHS staff identified a list of potential authorities that may or may not apply, they told us they were not able to specify whether their agency had clear or specific authority to require telecommunications providers to take actions to address congestion, such as reducing customer transmission speeds or blocking entertainment Web sites. Instead, DHS's approach would be to assess the authorities as part of the development of any such strategy. While this approach could help DHS determine at some point if it or some other relevant federal agency had adequate authority to address potential Internet congestion, it would increase the risk that the federal government will not be able to respond rapidly or effectively if a pandemic quickly emerges.

Other federal government agencies might have authority to direct providers to take certain actions during a pandemic, but whether these are adequate is uncertain. Under the Communications Act of 1934, as amended (the Act), FCC has authority to regulate the telecommunications providers specifically and has authority generally with respect to interstate and foreign communication by wire and radio. According to FCC staff, there may be actions the FCC could take regarding the Internet to address threats to national security or public safety. However, in commenting on a draft of this report, FCC officials noted that there is an ongoing court challenge to FCC's authority regarding the Internet. In addition, FCC staff were not sure whether FCC would have sufficient authority to require private sector organizations to take all actions that may be deemed necessary in an emergency situation to relieve congestion and facilitate commerce, including teleworking by financial sector employees. As part of preparing a national broadband access plan, FCC has recently sought public comments on options for prioritizing Internet traffic in a pandemic.[31] According to FCC staff, very few comment letters addressed the prioritization issue. Based on our review, some service providers expressed interest in the government considering including a prioritization scheme in the plan. Additionally, one provider suggested the plan should

[31]Federal Communications Commission, *In the Matter of A National Broadband Plan for Our Future Notice of Inquiry*, GN Docket No. 09-51 (April 2009).

give providers flexibility to actively manage networks during a pandemic.[32] Finally, one financial sector organization noted that the plan should include a prioritization scheme to prioritize Internet traffic based on how critical it is to national and economic security.

Some observers have suggested that an authority granted to the President in the Communications Act of 1934 could conceivably be used to take actions to address Internet congestion during a pandemic.[33] In their view, the President may have, under certain limited circumstances involving a state or threat of war, the power to authorize government control of the telecommunications systems and, if properly invoked and delegated, this might broadly provide authority for the government to require private sector entities to take actions intended to address congestion. However, according to FCC staff we spoke with, while the authority under the Act may grant the President powers over telecommunication systems during wartime, they did not know whether such powers could be exercised in a pandemic. However, until DHS, as the lead agency responsible for coordinating protection of telecommunications, including the Internet, takes action to work with other agencies to assess whether sufficient authorities exist to direct necessary actions by the private sector, the potential for a timely and effective federal response to congestion is reduced.

Voluntary Reductions in Internet Use May Be an Effective Response to Congestion, but DHS Has Not Taken Steps to Encourage It

Although its own study identified voluntary public reduction of Internet use as an effective means of reducing pandemic congestion, DHS has not begun steps to assess the feasibility and effectiveness of obtaining such public cooperation. According to the DHS study and to providers and others we spoke with, voluntary actions taken by the general public could have significant potential to reduce the surges in traffic loads that residential users may experience during a pandemic. For example, the general public could be asked to limit video streaming, gaming, and peer-to-peer and other bandwidth-intensive applications during daytime work hours. They could also be encouraged to use broadcast news sources in

[32]At the time of our review, FCC had received over 10,000 comments. We searched FCC's Electronic Comment Filing System for comments that were filed on behalf of certain telecommunication and cable providers and communication and financial sector organizations using terms such as priority, pandemic, and public safety as our search criteria. If our search resulted in a record for a specific provider or organization, we reviewed these excerpts.

[33]*See* 47 U.S.C. § 606.

place of online news. A similar campaign developed by another agency—HHS—to publicize pandemic awareness strategies showed that such public education efforts can require months to prepare and cost millions of dollars to test and implement. For example, as part of creating various radio and television messages to provide information to the public about how to prepare for a pandemic, HHS conducted market research using various techniques, including focus groups, to gauge the public's opinion about a pandemic. In 2005-2006, when they began this effort, HHS staff stated that it took the agency about 6 months to develop the public service announcements (PSA). In 2006-2007 HHS staff spent about 4 months planning and producing PSAs. The cost of running radio PSAs in 137 cities over an 11-month period in 2007 was about $1.5 million dollars.

DHS staff acknowledged that such a campaign would also require cooperation and coordination among multiple federal and other agencies to be effective and avoid conflicting goals and activities. For example, agencies would need to work together to ensure that some were not planning to recommend increased use of the Internet to provide information, education, or for other purposes during a pandemic. For example, HHS may advocate using the Internet to maintain social ties during a pandemic, which would make the goal of easing congestion by staying off-line more challenging. However, DHS staff told us they had not begun efforts to evaluate the feasibility or effectiveness of such a campaign or taken steps to begin developing such an effort because other activities supporting its operational mission have taken priority. Until DHS takes such action, its ability to implement what its own study predicted would be an effective tool for reducing potential Internet congestion in a timely fashion is reduced.

Key Securities Market Participants Have Prepared Response Plans, but Not All Have Documented Staffing Analyses or Plans for Alternatives to Teleworking

We reviewed seven organizations whose operations are critical to the overall functioning of U.S. securities markets and found that all have developed formal plans that address key elements of pandemic preparedness. But some have limitations that could increase the risk that aspects of their operations would be disrupted by a pandemic. In response to our last report, SEC and the banking regulators issued guidance to key financial market participants stipulating that an institution's pandemic plan, at a minimum, must include the following five key elements:[34]

1. a process for monitoring the pandemic's progress and a series of escalating response steps as various pandemic phases are reached;
2. a preventive program to minimize, to the extent possible, illness among employees, including social distancing of employees by curtailing meetings;
3. a documented strategy of facilities or procedures designed to allow the organization to continue its critical operations in the event that large numbers of its staff are unavailable for prolonged periods;
4. a testing program to better ensure that the practices and capabilities that an organization implements to address a pandemic will be effective and allow it to continue its critical operations; and
5. an oversight program to ensure ongoing review and updates to the pandemic plan.

All Seven Critical Organizations Have Escalating Plans and Preventive Programs

All seven of the critical financial market organizations we reviewed have developed formal pandemic plans that call for them to monitor a pandemic's progress and take escalating steps as the phases of a pandemic outbreak progress. Health authorities, including WHO and CDC, have issued phased timelines that track the progress of a pandemic from

[34]Of the seven critical organizations, five are overseen by SEC and two are under the purview of the banking regulators. The guidance issued by SEC was a letter to the organizations, not a formal rule, but the organizations were expected to comply with its requirements by year-end 2007.

earliest detection to widespread global illness.[35] Because being able to operate effectively at the height of a pandemic could require an organization to have taken steps in advance, an effective pandemic plan should contain more and stronger measures that would be taken as the phases of the pandemic progress. Such a strategy provides sufficient time to take steps that require more planning or lead time, such as purchasing needed supplies or conducting training in advance of the actual pandemic. Gradually implementing responses as the pandemic progresses also could prevent organizations from generating undue expenses if what appears to be a pandemic early on does not turn out to be one that significantly disrupts operations.

Our analysis of the seven critical organizations' pandemic plans showed that each included activities that escalated as the pandemic progressed. All the organizations are currently monitoring the information regarding the potential spread of viruses that could lead to a pandemic through the CDC or WHO Web sites and communicate closely with local authorities, such as the New York City Office of Emergency Management. In the early stages of a pandemic these organizations would take preventive actions, such as monitoring the world pandemic situation and creating awareness of wellness practices before widespread outbreaks begin (i.e., WHO Phases 1 through 3). But as the pandemic levels advance, the organizations' plans generally call for them to implement more extensive responses, such as relocating staff to increase social distancing or sending some staff home to telework. For example, one organization's pandemic plan describes efforts to impose business travel restrictions; prepare

[35]WHO defines the phases of increasing public health risk associated with the emergence of a new influenza virus and tracks the status of virus transmission using a six-phase scale. The interpandemic period includes WHO Phases 1 and 2; the pandemic alert period includes Phases 3, 4, and 5; and the pandemic period is WHO Phase 6. Specifically, WHO Phase 1 exists when no new influenza virus subtypes have been detected in humans. WHO Phase 2 occurs when a circulating animal influenza virus subtype is identified that poses a substantial risk of causing human illness. WHO Phase 3 is reached when a human infection with a new subtype is identified but no human-to-human spread is occurring. WHO Phase 4 is reached when small clusters of limited human-to-human transmission are occurring. WHO Phase 5 is reached when large but localized clusters of human-to-human spread are occurring. Lastly, WHO Phase 6 is a pandemic occurring with increased and sustained transmission in the general population. The U.S. Government Stages, first published in the *National Strategy for Pandemic Influenza Implementation Plan* (2006) also changed in accordance with the spread of the disease. HHS officials indicated that the U.S. Government Stages were therefore not appropriate to use in measuring the H1N1 outbreak of 2009, due to its low lethality, and removed the Stages from the government's Web site, www.flu.gov. HHS officials told us they do not have plans for revising the U.S. Government Stages at the time of this report.

additional communications to employees, customers, and regulatory bodies; and stock up on additional critical supplies during WHO Phase 4 in case a pandemic disrupts supply chains. As the alert level rises to Phase 5, the plan escalates the actions to initiate daily absenteeism tracking, expand the deployment of hand-sanitizing gel, and do additional facility cleaning. When WHO declares a pandemic (i.e., WHO Phase 6), the organizations will take steps to implement social distancing, such as sending a number of employees to the backup facility and designating people to work from home. All of the plans follow this general design, and during the H1N1 outbreak, all the organizations began implementing some of these steps. In particular, as the alert level escalated from WHO Phase 4 to Phase 5 in April of 2009, several organizations communicated to staff on additional measures they were taking, which included placing more hand sanitizers in the workplace and cleaning facilities more often. As WHO raised its pandemic phase further to the highest level (i.e., WHO Phase 6), indicating that a broad outbreak of an influenza epidemic was believed to be imminent, organizations, according to SEC staff, were prepared to take further steps that correspond with an outbreak—such as performing medical screenings of staff reporting to work—although such measures ultimately were not necessary due to the milder nature of the H1N1 outbreak here in the United States.

As a result of their experiences with the recent H1N1 flu outbreak, some market organizations and financial regulators told us they were considering developing modified trigger points in the plans that might not follow the WHO designations exactly. Officials from these organization said they had made this decision because of their experience with the relatively benign nature of the H1N1 virus in the United States. The health authorities' pandemic phases were designed for a disease that causes high levels of severe illness, and even deaths, like some of the previous flu pandemics have caused. However, even though the United States continues to report the largest number of novel H1N1 cases of any country worldwide, most people who have become ill in 2009 have recovered without requiring medical treatment. As a result, staff from several of the critical market organizations did not need to fully implement their plans at that time because their employees were not seriously ill, if at all, and the plans could be modified to adapt to such a scenario.

Our analysis indicated that all seven critical organizations also had fully addressed another key element of pandemic planning by instituting preventive programs intended to reduce the impact of a pandemic on their organizations. Because an organization has a much greater chance of continuing operations during a pandemic if fewer of its employees are ill,

an effective pandemic plan should include a preventive program to reduce the likelihood of employees becoming sick. The steps the organizations took included providing information and educational campaigns to keep employees informed of pandemic news and developments. For example, during the recent H1N1 outbreak, staff at these seven organizations developed memos to employees on the status of the outbreak and steps the organizations were taking based on news and briefings from the federal, state, and local authorities. Further, all the organizations have developed internal Web sites to educate employees on general information on preventing spread of disease, including hand-washing techniques and coughing etiquette and provided personal hygiene items such as hand sanitizers and masks. In addition, three of the organizations prepared extensive education outreach campaigns (e.g., hand-washing awareness week) shortly after the financial regulators' pandemic planning requirements were issued, in mid-2007. Most of the organizations have also developed policies regarding restricting travel as a way to reduce illness among their employees. For example, the organizations' plans typically called for curtailing international travel at WHO Phase 4, and some required staff returning from abroad to quarantine themselves for a period, such as 7 days, to lower the chance of spreading illness.

Critical Organizations Reviewed Have Plans to Continue Operations with High Absenteeism, but Some Have Limitations in Their Staffing Plans and Teleworking Alternatives

All seven critical securities market organizations we reviewed have developed plans with procedures intended to allow them to continue the functions critical to their operations despite high levels of absenteeism, but not all have fully analyzed or thoroughly documented their staffing levels or developed formal alternatives if teleworking proves unfeasible due to Internet congestion. Although congestion during a pandemic could interfere with individuals' ability, including teleworkers and others, to access the Internet, the primary communications of the critical markets organizations would not be affected because these organizations and their participants communicate via high-capacity, proprietary networks that do not traverse the public Internet infrastructure.[36] According to the health authorities, one of the most significant challenges of a pandemic will be

[36]For example, stock and options exchanges receive trade orders from broker-dealers over the Secure Financial Transaction Infrastructure, which is a network created to provide a more reliable and "survivable" private communications network that links exchanges, clearing organizations, and other financial market participants. This network employs redundant equipment throughout, and carries data traffic over redundant fiber-optic rings that have geographically and physically diverse routes. The clearing organization for stocks has set up a similar proprietary network.

staffing shortages due to absenteeism caused by employees either too ill to work, taking care of ill family members, or afraid to come to work because of the chance of infection. Unfortunately, organizations could also permanently lose critical staff if the pandemic causes significant levels of deaths. Therefore, a responsive pandemic plan should include procedures for ensuring that an organization can continue performing its critical functions even with as much as a 40 percent reduction in its workforce for a prolonged period—the level that the federal government has advised should be used for planning for a severe pandemic.

In general, the seven critical organizations that we reviewed all intend to use existing geographically dispersed facilities to increase the distance among staff who perform critical functions. Staff from all seven critical organizations are spread among facilities located across the United States, including data centers, which are monitored by computer operators, and office or business centers with key staff that assist customers. Each of these organizations has created duplicate sites with redundant staffed data centers and locations or space for other critical staff. For example, officials from one organization told us that their three facilities are considerably distant from each other (i.e., hundreds of miles) in order to mitigate the effect of natural disasters, power and telecom outages, and other wide-scale regional disruptions, including a pandemic. The organizations plan to use these geographically dispersed sites to maximize social distancing and increase their ability to continue operating during a pandemic. Having sites with staff that perform critical functions in more than one location also provides these organizations with pools of cross-trained employees that they can draw on during a pandemic. For example, one organization's pandemic plan relies on staff performing critical activities that are evenly divided across two geographically distant facilities in different regions of the country. This organization also has an alternate facility in the same metropolitan area as its primary location. Under its plan, during the final stage of a pandemic, when the United States is experiencing sustained transmission of the disease, some staff from its primary site are to report to the nearby alternate facility to do their critical activities, thus allowing the organization to increase the physical distance between the individual members of its critical staff.

Staffing Analyses or Documentation Can Be Improved

Although each organization has developed plans for continuing operations during a pandemic, our analysis indicated that three of the seven have not fully analyzed or documented the number of staff able to perform critical functions who would be available during a pandemic. With the federal government indicating that organizations should plan for absenteeism of 40 percent at the peak of a severe pandemic, under such circumstances

approximately one in every three of an organization's employees could be ill or caring for ill family members. Although regulators' guidance does not specify the extent of cross-training required, we believe that, at a minimum, an organization would need two staff capable of performing each critical activity to allow for one to be absent while the other continues working. Organizations should probably have three staff capable of performing or cross-trained to take over these tasks to provide additional assurance that enough staff would be available. For example, the federal guidance on continuity of operations planning recommends that organizations should probably have three staff capable for key positions.[37]

Because these organizations have multiple operating sites with staff located in each that are capable of performing many of their critical activities, they have some assurance that they likely have enough employees to continuing operating during a pandemic. But, not all organizations have fully analyzed or documented the number of staff that could be available across all critical positions and tasks. All the organizations have identified their critical functions and all have lists of at least some of the essential staff for each of the departments performing those functions. Four critical organizations have developed lists that show the current staff for each critical function, backup staff, and sufficient numbers of staff who are cross-trained or already know these functions who could serve as additional backup support. One of these organizations rotates the performance of its critical functions through three geographically distant operation sites on an ongoing basis, ensuring a large group of cross-trained staff. For example, this organization has a list of 36 staff for one of the critical departments, all of whom are trained to perform functions normally requiring 8 staff. Thus the organization has 8 backup staff as well as 20 additional trained staff that it can draw upon. Another of the four organizations identified seven essential services that its organization needs to perform and prepared listings for each of these departments that identify the primary staff performing the functions, the backups for these staff, and additional staff that are knowledgeable or cross-trained to perform these duties. For example, one of the essential departments has a list of 19 staff that are trained to perform one set of critical functions that normally require only 5 employees—a surplus of 14. In addition, this organization cross-trained an additional 7 staff to serve as

[37] *Federal Guidance To Assist States In Improving State-Level Pandemic Influenza Operating Plans* (March 2008).

further backup support. Henceforth, these organizations identified additional staff beyond the primary and backup employees for each critical function—producing more than two staff capable of performing each critical activity—to have greater assurance of being able to perform their critical functions.

The importance of sufficiently analyzing and documenting the adequacy of critical staffing was demonstrated by one of the critical organizations that has comprehensively identified its staff and backups. This organization participated in an industry-wide pandemic exercise that revealed it needed to identify even larger numbers of trained staff for some departments. The exercise simulated the impact of a pandemic by declaring that all staff with last names beginning with certain letters would be unavailable for work. Although at one point in the exercise the scenario called for 40 to 50 percent absenteeism, this organization found that in one of its critical departments, as many as 78 percent of its staff were projected to be unavailable.[38] As a result, this organization has re-examined its staffing arrangement to identify staff that currently perform other activities that could be used to perform critical functions if needed. The results from the exercise demonstrated the need to determine, in advance of an outbreak, sufficient numbers of staff capable of performing critical functions.

In contrast, three of the seven critical organizations have not fully developed lists of staff capable of performing critical functions. For example, at one organization each critical department listed essential staff, but only at a managerial level (e.g., vice president of a department, and one backup) but did not identify staff that perform the department's functions on a day-to-day basis. The other two organizations created lists of essential staff by department, but the lists were completed only during the recent H1N1 outbreak rather than in advance. None of these three organizations listed primary, backup, or other staff for the critical functions. Officials at one of these organizations told us they have staff at several geographic locations and that business continuity tests for one of their critical departments demonstrated they can operate their organization's critical information systems. As a result, they said that the geographic distance among locations and testing efforts provided them with a group of cross-trained staff that would be sufficient to continue

[38]This absenteeism model uses the first letters of employees' last names, relying on U.S. Census figures for the distribution. This method provided a realistic picture of the range of absent employees, which could be from the lowest levels to the top of an organization.

operations even if 40 percent were absent. While this provides some assurance that this organization may be able to withstand a pandemic, as one organization learned, undergoing more extensive analysis and documentation allows organizations to identify gaps in staffing levels that would be unique to a pandemic, when large numbers of staff could be unavailable for prolonged periods. In addition, such analyses identify all critical tasks and those staff capable of performing them—primary, backup, and additional cross-trained staff—providing these organizations with greater assurance that adequate numbers of staff exist for each task within its critical departments. Until these organizations fully document their staffing analyses to ensure they have sufficient depth of staff capable of performing critical functions, some aspects of these organizations' operations may be affected during a pandemic.

Alternative Strategies to Teleworking Should Be Considered

In addition to better analyzing and documenting their staffing plans, some of the organizations that intend to use teleworking as part of their strategy for continuing operations during a pandemic need to address limitations in their teleworking plans. As noted previously, the critical market organizations included in our review generally rely on proprietary communications networks that will not likely be affected by any pandemic-related congestion. However, five of the seven critical organizations plan to have some of their critical staff telework during a pandemic, and the readiness of these organizations to successfully have employees telework varies. Based on our reviews, only one of the five organizations fully developed suitable alternatives to teleworking in case of Internet congestion. This organization identified hotels with increased broadband Internet access capability in the employees' residential neighborhoods that staff could report to in order to improve their ability to telework. Another of the five organizations developed a plan for some of the critical staff that would be teleworking to come into one of its facilities that is currently prepared as a backup site. This facility is currently ready for operations and has ample space to provide adequate social distance for employees that find they cannot successfully telework due to congestion. However, the organization has not made adequate preparations for some critical staff in another geographic area to telework during a pandemic. If these employees are not able to telework, the organization plans to have them report to its office there and work in an unused part of the facility. But it has not outfitted this area with additional workstations that would allow its staff to work there effectively.

Furthermore, three of the critical organizations whose plans include possibly having some of their critical employees telework have not fully developed plans for alternatives to teleworking should congestion arise.

Our review of their plans show that the three organizations have not designated the necessary positions or employees who would telework. Determining the total number of teleworkers in advance of an outbreak would allow the organizations to confirm that their network systems can fully support that number, which would likely be higher than it might be in the course of a normal work day, and that these employees have full access to all the applications or systems they need in order to perform their critical duties effectively from home. These organizations have also not developed and assessed the feasibility of alternatives to teleworking in their plans. For example, one of these organizations told us that, if congestion occurs, they would bring staff back into their facilities and have them conduct their work wirelessly. However, they have not documented this in their planning or tested the feasibility of this approach for all potential critical activities. The other two organizations have not determined in their plans what steps they would take to respond to congestion problems experienced by their teleworking employees. Until all the critical organizations develop additional measures to ensure they have viable alternative strategies if teleworking proves difficult, they might be at greater risk of having some aspects of their operations disrupted during a pandemic.

Critical Organizations Reviewed Have Tested Plans and Ensured Ongoing Review to Varying Extents

Our analysis shows that while all seven of the critical organizations we reviewed participated in an industry-wide pandemic scenario test, some have not conducted similar tests internally. All of the organizations reported that they participated in a 3-week industry-wide pandemic exercise, sponsored jointly by FBIIC, FSSCC, Treasury, and the Securities Industry and Financial Markets Association, which began in September 2007.[39] The exercise simulated a pandemic occurring in three waves and

[39]The Financial and Banking Information Infrastructure is chartered under the President's Working Group on Financial Markets and is charged with improving coordination and communication among financial regulators. The Financial Services Sector Coordinating Council is a group of over 30 private sector firms and financial trade associations that works to help reinforce the financial service sector's resilience against threats to the nation's financial infrastructure. The Securities Industry and Financial Market Association is a nonprofit organization that brings together the shared interest of more than 650 securities firms, banks, and asset managers. Its mission is to promote policies and practices that work to expand and perfect markets, foster the development of new products and services, and create efficiencies for member firms.

reaching an absenteeism rate as high as 49 percent.[40] As previously mentioned, each scenario update included an absenteeism distribution specified by first letters of employees' last names, as a way to approximate the scenario's target absenteeism rate. The scenario updates were provided to participants 1 week in advance so that each organization had adequate time to review its human resources records, identify the absent individuals, and determine the distribution of the absent employees among their various departments and units as appropriate. This method provided a probable picture of the range of absent employees, which could be from the lowest levels to the top of an organization. Organizations that did not want to carry out such a review of their records were allowed to simply use the provided absenteeism rate (25 percent, 49 percent, and 35 percent) for each scenario update.

Officials from the critical organizations indicated that the exercise was useful in planning for a possible pandemic. As noted previously, one organization participating in this exercise experienced as much as 78 percent absenteeism in some of its departments—higher than the expected 49 percent projection—and has taken steps to identify additional staff capable of performing its critical functions. Officials from another organization said the exercise highlighted variation in human resource policies—for example, in the distribution of antiviral medication and the use of hazard pay across regional offices. As a result, the organization convened relevant staff to discuss consistent policy issues and infrastructure resiliency across regions. In addition to the industry-wide effort, three of the organizations have conducted or plan to conduct additional internal pandemic tests to ensure readiness. One of the organizations has conducted pandemic exercises for managers and staff at each facility, using a set of questionnaires corresponding to various scenarios. Another organization told us that it planned to conduct a full-day pandemic response test at all of its facilities in 2009. However, four of the organizations have not run internal pandemic scenario tests. As discussed earlier, the results from the industry-wide test demonstrated the need for the critical organizations to assess their staffing, backup, and

[40]Spread of the pandemic scenario for the exercise is described as follows: At the start of the prephase scenario, clusters of a highly human-to-human transmissible strain of the H5N1 virus were confirmed in Africa, the Middle East, Europe, and South Asia. By 6 weeks (scenario update 2), the virus had reached pandemic levels across the United States, and corresponding absenteeism rates reached a peak of 49 percent. Eight weeks later (scenario update 3), the United States and other areas affected early in the pandemic were entering a recovery period, and the number of reported cases began to peak in South America, northeast Asia, the Pacific, and the Australian continent.

cross-training levels to ensure they are sufficient to meet the organization's needs during a pandemic. Internal pandemic scenario tests would give organizations just such an opportunity.

In addition to pandemic scenario testing, all seven organizations have tested their abilities to run critical applications and functions at their alternate backup facilities as part of their business continuity testing. These efforts will provide further assurance that these sites will be viable for use during a pandemic. Some of the organizations rotate operations between the primary and the backup facility on a regular basis, while others operate certain processes simultaneously at the primary and the secondary facilities. For example, one of the organizations conducts six remote-site recovery tests per year, simulating failure of applications. Meanwhile, another organization has begun recovery testing by alternating its full production cycle between the two key facilities. Further, all but one of the five firms that intend to employ teleworking as part of their pandemic plan have assessed their work-from-home capabilities—an essential part of planning for extensive teleworking to ensure that the organizations' telecommunications systems can support the large amounts of traffic that would be generated. One organization in particular tested work-from-home infrastructure to ensure continuity of daily production as early as mid-2007 and continues to test connectivity as its telecommunications infrastructure is upgraded. Another organization told us it conducted several work-from-home tests in 2008, including server stress test and tests featuring full-volume transaction levels. This kind of testing is critical to pandemic planning, especially for those organizations that intend to have some of their critical staff work from home.

Our analysis also indicates that six of the seven of the organizations have procedures in place to ensure their pandemic plans are being reviewed and updated. Because pandemic plans should be sufficiently flexible to effectively address a wide range of possible effects that could result from a pandemic, ongoing review and updates will ensure a plan has up-to-date policies, standards, and procedures. Officials from the six organizations told us that the pandemic plans are reviewed on a regular basis, either at the business-department level or in some cases by the audit committee or the Board of Directors. For example, at one organization the audit committee reviews the pandemic plan and reports its assessment and findings to the Board of Directors on an annual basis. At another organization, the departmental plan is prepared by the department manager and is approved by the director. However, at one organization executives have seen the pandemic plan, but it has not been formally approved. This organization told us it recently instituted a pandemic flu

committee that will formally review and approve the pandemic plan. Regular review and approval by senior management helps to ensure that adequate resources are dedicated to implementing the plan. Furthermore, with the changes occurring across financial organizations due to the recent market turmoil, regular review helps an organization confirm that its plan is still aligned effectively to its organizational structure.

SEC Has Taken Significant Steps to Assess Securities Market Organizations' Pandemic Preparedness, but Could Do More

As the regulator that oversees stock and options exchanges, clearing organizations, and broker-dealers, SEC has taken various actions to ensure that market organizations are preparing for a pandemic, including issuing guidance and conducting examinations of market participants' preparations, but could take additional steps to better oversee firms' readiness.[41] To ensure the readiness of the participants in the securities markets, SEC has issued various communications that provided guidance outlining its expectations for these entities' pandemic preparation efforts. For example, in April 2006, SEC sent a letter to securities exchanges and clearing organizations advising them to plan for a pandemic and make preparations intended to keep the markets operating. SEC's letter noted that the organizations' existing business continuity programs were usually designed to address a discrete event and therefore could prove inadequate to address the potentially long-lasting impact of a pandemic. SEC staff also spoke at conferences, meetings with market participants, and other forums, such as those sponsored by industry trade associations, to share information about pandemic issues. Although securities regulators had taken various actions to help the financial markets prepare, our 2007 report indicated that additional actions could further improve the financial market's readiness to withstand an influenza pandemic.[42] In response to our recommendation, SEC provided more specific guidance between July and October 2007 to the securities exchanges, clearing organizations, and broker-dealers that indicated that these organizations' pandemic plans

[41]The banking regulators, who oversee the clearing banks that maintain accounts on behalf of securities market participants, have taken similar actions. Given that our review of the pandemic plans of the two critical market organizations overseen by the banking regulators indicates that these organizations have plans that meet the required criteria without limitations, we did not assess the banking regulators' activities related to pandemic preparedness. Furthermore, we did not conduct on-site independent reviews to verify the bank regulators' assessments of banks' readiness. However we did interview banking regulators about their supervisory efforts in the area of pandemic preparedness, and present that information in appendix III.

[42]GAO-07-399.

include various key elements, such as procedures for continuing operations during even severe pandemics, and that the plans be in place by the end of 2007.

To ensure that securities market organizations are taking adequate steps to be ready for a pandemic, SEC has been conducting examinations of various market participants' preparations that cover, among other things, pandemic preparedness plans. To assess the extent to which securities exchanges, electronic markets, and clearing organizations are adequately managing risks to their operations, staff from SEC's Division of Trading and Markets regularly conduct examinations through its Automation Review Program (ARP).[43] Since beginning this program in the late 1980s, SEC has issued guidance and conducted examinations that address operations risk issues at these organizations, including reviewing physical and information security and business continuity planning. As of September 2009, 22 securities exchanges, electronic markets, and clearing organizations were subject to ARP's guidance and examinations, including five of the organizations whose operations we consider critical to the securities markets.[44]

As part of the ARP examinations, SEC staff have been addressing these organizations' pandemic preparedness during their reviews of business continuity issues. During these examinations, SEC staff were using an examination module, adapted from the Federal Reserve, to assess whether these organizations have developed plans that adequately address the five key elements of a pandemic plan, including whether the organizations identified their critical staff, had procedures for reducing the likelihood of their staff becoming ill, and tested their plans. From January 2007 to June 2009, SEC's Division of Trading and Markets staff had conducted nine examinations addressing business continuity planning and pandemic preparedness at the critical organizations included in our review. Although examiners generally found in the 2007 examinations that organizations were in various stages of pandemic preparations, and in some cases had

[43]SEC published its Automation Review Policy in 1989, to oversee the operational risks at the securities exchanges and clearing organizations. The Policy advised self-regulatory organizations prospectively of SEC's expectations on how these organizations should address information dissemination and physical security and business continuity challenges. Automated Systems of Self-Regulatory Organizations, Securities Exchange Act Release No. 34-27445, 54 Fed. Reg. 48703 (Nov. 24, 1989).

[44]The other two of the seven organizations that we consider critical to the market are under the purview of the banking regulators.

not addressed all the required elements of a pandemic plan, our review of the examination reports that SEC conducted in 2008 and 2009 indicate that these organizations improved their plans to better address the key elements of pandemic preparedness. However, after examining one of the organizations in October 2008, SEC staff made various recommendations to direct this organization to improve its pandemic planning. For example, SEC recommended that the organization's plan better address the impact of staff reductions on its operations and that it test its pandemic procedures.

SEC Examinations of Organizations' Staffing Analyses Could Go Farther

Although SEC has conducted inspections to ensure that critical organizations are preparing plans that address all the key pandemic areas, SEC's examination reports did not always cite as deficiencies the limited analysis or documentation of these organizations' staffing levels. The pandemic assessment questions used by SEC staff addressed issues related to staff dependencies, including whether the organizations identified their key functions and staff for these functions and conducted cross-training of staff to ensure that sufficient staff would be available during a pandemic. However, as noted earlier, our reviews of the critical market organizations indicate that three of the five critical securities market organizations have not adequately documented the number of staff who could perform critical functions if many of the staff that currently perform those functions are unavailable during a pandemic. Our reviews of SEC's examination reports show that SEC staff identified weaknesses in the staffing analysis at one of these critical organizations but not at the other two. SEC staff acknowledged that ensuring adequate numbers of critical staff is important. But they said they had not expected the organizations to document the adequacy of their staffing for all their positions because staff in critical departments were likely to be interchangeable and thus could fill in for each other. Moreover, in their opinion, specific staffing lists could quickly become out of date given the higher rate of staff turnover at these organizations during this current financial crisis.

Although we agree that the critical organizations may have staff throughout their organizations that could step in for ill employees during a pandemic, until such staffing depth is better assessed and documented, these organizations cannot be fully assured of their ability to operate during such an event. As we noted previously, even organizations that created listings of the staff capable of performing critical functions found during testing that what they thought was sufficient depth in staffing was actually inadequate in some departments. In addition, this current period

of increased staff turnover among financial organizations likely further increases the risk that an organization could have thinner staffing for some key positions that might not be identified until a pandemic is occurring. As a result, until SEC staff take steps to ensure that these organizations better document the adequacy of the depth of their critical function staffing, some aspects of these organizations' operations could be disrupted during a severe pandemic.

SEC Examinations of Teleworking Could Address Alternatives

Although SEC's ARP staff's reviews address the extent to which the critical organizations plan to have employees telework during a pandemic, their examinations thus far have not included checking for viable alternate strategies if Internet congestion occurs. SEC staff told us that as part of their pandemic examinations at securities market organizations, they were reviewing various teleworking issues by addressing the relevant questions in their examination module regarding whether the organizations had remote access arrangements and whether the organizations had assessed the capacities of their communications links. The SEC module also asks whether an organization analyzed the locations of its staff's homes to see if there were large numbers of staff that may be trying to connect from a single area and thus be more vulnerable if congestion or disruption occurs in that area. However, neither the SEC staff's examination module nor the examination reports we reviewed address whether these organizations developed formal plans for what to do with their teleworking staff if congestion prevents that strategy from being viable. As noted earlier, our reviews of the critical organizations indicate that not all have developed adequate alternative strategies in the event that staff are unable to telework effectively. Until SEC staff take steps to ensure that all organizations develop such strategies, the risk exists that a pandemic could disrupt some areas of these organizations' operations.

SEC Has Also Taken Steps to Assess the Pandemic Preparedness of Some Broker-Dealers

In addition to taking steps to assess the readiness of securities exchanges, electronic markets, and clearing organizations to continue operating during a pandemic, SEC staff have been reviewing the preparations of large broker-dealers whose activities are important to overall market functioning. In the aftermath of the September 11, 2001 terrorist attacks, SEC and the banking regulators made coordinated efforts to ensure the resiliency of the U.S. securities markets with respect to clearance and settlement activities. As the attacks showed, the inability of individual securities market participants to promptly clear and settle transactions can pose significant financial risks to other participants. In response, SEC, the Federal Reserve, and the Office of the Comptroller of the Currency

jointly issued the Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System (Sound Practices) in April 2003.[45] The Sound Practices paper establishes business continuity expectations for the clearance and settlement activities of organizations that support critical financial markets. These organizations include the core clearing and settlement entities that process securities transactions (core organizations) and firms that play a significant role in critical financial markets (significant firms)—generally defined as those firms whose participation in the markets results in their consistently clearing or settling at least 5 percent of the value of the transactions in any of the product markets specified in the paper.[46] Since issuing the paper, these regulators have been conducting examinations of the clearing organizations, significant broker-dealers, and clearing banks that are subject to these practices to ensure they have in place business continuity arrangements sufficient to meet various recovery goals for their clearance and settlement activities.[47]

All of the recent examinations that SEC staff conducted under the Sound Practices effort also addressed the pandemic preparations for the significant number of broker-dealers whose role in the critical financial market activities were deemed significant for selected securities and other product markets. In early 2008, staff in SEC's Office of Compliance Inspections and Examinations, which is responsible for conducting examinations of broker-dealers, mutual funds, and investment advisers, conducted reviews of the then-largest existing broker-dealers. Because of these entities' high trading volumes in various securities or other products, the markets could be significantly affected if they were unable to clear and settle their transactions. As part of these reviews, SEC staff obtained documentation on how these broker-dealers were addressing the key elements of pandemic planning. Based on these assessments, SEC staff found that the largest broker-dealers appeared to be implementing

[45]68 Fed. Reg. 17809 (Apr. 11, 2003).

[46]"Core clearing and settlement organizations" include government or private sector entities that provide clearing and settlement services that are integral to a critical market. Among the specific product markets included in the paper are those for government and corporate securities, commercial paper, foreign exchange, and others. *Id.* at 17811.

[47]Core clearing and settlement organizations are to strive to recover these activities within 2 hours of a disastrous event, and significant firms are to strive to recover these activities within 4 hours. *Id.* at 17812-17813.

pandemic plans that generally addressed the key elements.[48] However, as part of conducting some operations risk examinations of a broader group of broker-dealers during 2008, SEC staff also examined the extent to which four midsized firms that cleared trades for other broker-dealers had begun preparations for a pandemic. During these reviews, SEC staff found that, unlike the larger firms, three of these four clearing broker-dealers had no formal pandemic plans in place.

FINRA Has Also Taken Steps to Assess Broker-Dealer Readiness for a Pandemic

In addition to the broker-dealers overseen by SEC, we also reviewed FINRA, the self-regulatory organization that oversees most broker-dealers in the United States. FINRA oversees broker-dealers, including "introducing" firms that accept customer orders and "clearing firms" that process introducing firms' orders. Prior to H1N1 and our inquiries, FINRA had not fully assessed the pandemic readiness of broker-dealers, including clearing firms. However, since then, FINRA administered a voluntary survey of significant firms, in which a majority of the firms reported they are engaged in some level of pandemic planning. The results of the survey will be used to identify areas for improvement moving forward, including a new examination module that addresses pandemic readiness. For further information on FINRA's activities, see appendix II.

Conclusions

The increased demand on the Internet resulting from the number of students, workers, and other family members at home during the day during a severe pandemic is expected to create congestion by exceeding the current capacity of Internet providers' network infrastructure in residential neighborhoods. Telecommunications providers will have limited options to expand network infrastructure during an outbreak, and possible network management techniques would likely require government action in order for providers to avoid violating existing customer service agreements. DHS is the federal agency responsible for working with the private sector to ensure that the critical communications sector, which includes the networks that comprise the Internet, is protected from attacks and other disasters. Although DHS has taken some actions relating to pandemic and possible Internet congestion, it has not

[48]Unlike the critical market organizations, we did not conduct on-site independent reviews to verify the SEC's assessments of the broker-dealers' readiness; for more on this, see appendix I.

taken the necessary steps to develop a strategy for addressing such congestion.

In addition, developing an effective Internet congestion response plan will likely require coordination with various other federal agencies, including the Department of Education, HHS, and FCC. As the experience of Hurricane Katrina showed, working in advance of a crisis to understand the proper roles and responsibilities of various federal and other entities is important for ensuring an effective response, but DHS has not taken extensive actions to coordinate with other relevant federal and private sector entities about actions that could potentially reduce Internet congestion and how best to respond. In addition, an important step for ensuring the federal government is prepared to address pandemic-related Internet congestion will be identifying whether any federal entity currently has the needed authority to take any actions determined to be necessary. However, whether DHS, FCC, or others have sufficient existing authorities to direct private sector Internet providers to take the actions necessary to relieve congestion is not clear. Similarly, although its own study showed that obtaining public cooperation in reducing nonessential use of the Internet could greatly resolve the potential pandemic-related congestion, DHS has not taken steps to assess the effectiveness and feasibility of mounting such a campaign to begin developing one. Until DHS develops an effective response strategy, coordinates with federal and other partners on actions to take, determines whether sufficient authorities to act exist or are sought, and evaluates the need for a public campaign, employees in critical sectors of the nation's economy, including those in financial services, might not be able to effectively telework or otherwise communicate or transmit data over the Internet during a pandemic.

Seven critical securities market organizations that we reviewed have taken significant steps to better ensure they would be able to continue operating during a pandemic, including by developing plans that address the key elements of pandemic planning. However, some of these organizations could better document the adequacy of their staffing levels and ensure they have prepared viable alternatives in the event that their teleworkers experience Internet congestion. SEC has taken various steps, including issuing guidance and conducting examinations, to ensure that financial market organizations, including those critical to the overall functioning of the markets, are prepared to continue operating during a pandemic. However, taking additional steps during their examinations to ensure that these organizations have fully documented the adequacy of their staffing analyses, developed formal alternatives to teleworking, and tested these

would provide greater assurance that the financial markets' full range of operations will not be disrupted by a pandemic.

Recommendations for Executive Action

To better ensure that securities market participants as well as organizations in other critical sectors of the economy will continue to have access to the Internet during a pandemic, we recommend that the Secretary of Homeland Security take the following four actions:

- develop a strategy outlining actions that could be taken to address potential Internet congestion,
- coordinate with other relevant federal and private sector entities about actions that could potentially reduce Internet congestion,
- work with other federal partners to determine if sufficient authority exists for one or more relevant agencies to take any contemplated actions to address Internet congestion, and
- assess the effectiveness and feasibility, and undertake if warranted, a public education campaign to reduce such congestion.

To better ensure that important securities market participants are making adequate preparations for pandemic, we recommend that the Chairman, SEC, ensure that SEC staff take steps to ensure that critical financial market organizations are fully documenting the adequacy of their staffing levels to withstand high absenteeism and have formally developed alternative strategies in the event that congestion limits teleworking effectiveness.

Agency Comments and Our Evaluation

We provided a draft of this report to the Secretary of Homeland Security, the Secretary of Health and Human Services, the Secretary of the Treasury, the Chairman of the Board of Governors of the Federal Reserve System, the Chairman of the Financial Industry Regulatory Authority, the Comptroller of the Currency, the Chairman of the Securities and Exchange Commission, and the Chairman of the Federal Communications Commission for their review and comment. In her letter, SEC's Chairman noted that she shares our concern that Internet congestion could impair certain aspects of the securities markets during a pandemic (see app. IV). She noted that she also agrees that critical market organizations can take steps to improve their existing pandemic plans. Accordingly, the Chairman indicated that SEC will issue letters to these organizations recommending that they further

document their staff cross-training arrangements and their plans to maintain operations if Internet congestion impairs their ability to rely on telework for support functions. Further, SEC staff will review compliance with this recommendation in future examinations of these organizations. The Chairman also noted that SEC is prepared to assist other agencies to help address the problem of potential Internet congestion.

In a written response to a draft of this report, the Director of DHS's Departmental GAO/OIG Liaison Office concurs in part with our recommendations that DHS should, among other things, develop a strategy outlining actions that could be taken to address potential Internet congestion. The Director's letter states that the agency agrees to take these steps to mitigate the impact of any pandemic-related congestion on the systems that the federal government uses to communicate critical national security/emergency preparedness (NS/EP) information, but that addressing Internet congestion for other communications, as a general matter, does not fall within DHS's responsibilities, and that DHS does not have the responsibility for developing an Internet congestion strategy separate and apart from assuring NS/EP communications. While we agree that DHS should ensure that NS/EP communications are maintained, DHS has been broadly tasked with leading efforts to prevent disruptions to the nation's overall telecommunications infrastructure and is the agency best positioned to do so. As discussed in this report, federal policies and plans assign DHS lead responsibility for facilitating a public/private response to and recovery from major Internet disruptions. DHS was designated under HSPD-7 as the lead agency for coordinating the protection of the communications sector—a role it plays for several of the other sectors that have been identified as the nation's critical infrastructures and key resources. As lead agency for this sector, DHS is to conduct vulnerability assessments and encourage risk management strategies to protect and mitigate against attacks. HSPD-7 also notes that agencies are responsible for working with their sectors to reduce the consequences of catastrophic failures not cased by terrorism. Similarly, the 2009 National Infrastructure Protection Plan notes that risk in the 21st century results from a complex mix of man-made and naturally occurring threats and hazards, including terrorist attacks, accidents, natural disasters, and other emergencies. Under this plan's risk analysis and management framework, sector-specific agencies are to combine consequence, vulnerability, and threat information to produce assessments of risks to a sector and enhance protection by setting goals and objectives, establishing priorities for mitigating risks, and implementing protective programs and resiliency strategies. Based on the study that DHS itself led, congestion resulting from a pandemic appears to be one of the threats for which DHS is tasked with ensuring an adequate governmental response. Furthermore, for

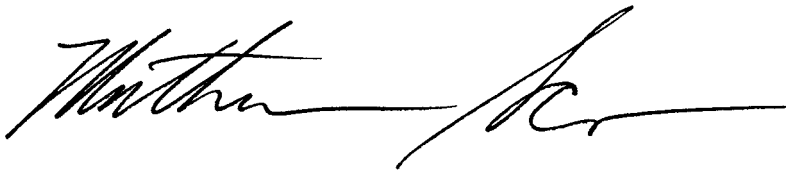
example, *The National Strategy to Secure Cyberspace* notes that the Internet is at the core of the information infrastructure upon which we depend, connecting millions of other computer networks and making most of the nation's essential services and infrastructures work. According to this strategy, DHS has important responsibilities to develop plans to secure these key resources and infrastructures and provide assistance to the private sector and other government entities with respect to recovery plans for failures in critical information systems. DHS has already been working to address threats to the Internet, for example, by establishing an Internet Disruption Working Group to work with the private sector to establish priorities and develop action plans to prevent major disruptions of the Internet and to identify recovery measures in the event of a major disruption. DHS also has an ongoing relationship with the communications sector coordinating council, which consists of various private sector telecommunications providers, that could assist in assessing and developing solutions to this issue. As a result of these responsibilities and its existing capabilities, we believe that DHS is the appropriate agency to take the lead in developing a strategy to address potential pandemic-related Internet congestion and to coordinate with other relevant federal and private sector entities about actions that could reduce such congestion.

DHS also commented that congestion that affects the Internet outside of NS/EP communications falls within the operational and administrative interests of other federal agencies. While we agree that other agencies, such as FCC, should play a role in addressing the potential negative impact on our nation's commerce and economy from pandemic-related Internet congestion, under the existing governmental policies, DHS is the agency that is specifically tasked with addressing threats that have the potential to disrupt the critical communications sector. Furthermore, this report notes the uncertainty that exists over whether FCC has the authority to act to address Internet-related congestion problems. The uncertainty of roles and authorities regarding this issue is the reason we recommended that DHS work with other federal partners to determine if sufficient authority exists for one or more relevant agencies to take any actions necessary to address Internet congestion that may occur during and because of a severe pandemic crisis. While other agencies could play critical roles in addressing this issue, we believe that DHS, as the communications sector lead agency, should provide this leadership and coordinate a response. The Director's letter also includes some additional technical comments that we address as appropriate in appendix V.

We also received technical comments from FCC and HHS, which are incorporated as appropriate in the report.

We are sending copies of this report to the Secretary of Homeland Security, the Chairman of the Securities and Exchange Commission, and other interested parties. The report will be available at no charge on the GAO Web site at http://www.gao.gov.

If you or your staff have any questions regarding this report, please contact Mathew Scire at (202) 512-8678 or sciremj@gao.gov; David Powner at (202) 512-9286 or pownerd@gao.gov; or Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix IV.



Mathew J. Scire
Director, Financial Markets and Community Investment

David A. Powner
Director, Information Technology Management Issues

Nabajyoti Barkakati, Chief Technologist
Director, Center for Technology and Engineering

List of Requesters

The Honorable Henry Waxman
Chairman
The Honorable John D. Dingell
Chair Emeritus
The Honorable Joe Barton
Ranking Member
Committee on Energy and Commerce
House of Representatives

The Honorable Barney Frank
Chairman
Committee on Financial Services
House of Representatives

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
House of Representatives

The Honorable Rick Boucher
Chairman
The Honorable Cliff Stearns
Ranking Member
Subcommittee on Communications, Technology, and the Internet
Committee on Energy and Commerce
House of Representatives

The Honorable Edward J. Markey
House of Representatives

Appendix I: Objectives, Scope, and Methodology

Our objectives were to determine (1) the potential impact of a severe pandemic on the Internet and the actions telecommunications providers and government agencies are taking to address possible congestion, (2) the adequacy of the actions that securities market organizations are taking to prepare pandemic plans, and (3) steps that securities and other regulators are taking to assess the readiness of securities market organizations to continue operating during a pandemic.

To describe the potential impact of a pandemic on the Internet and the actions that communications providers and relevant government agencies are taking to address possible congestion, we interviewed staff from two communications providers and two cable providers that are among the largest providers of Internet access service in the United States, as well as two industry associations representing such providers. In addition, we interviewed relevant officials at the Department of Homeland Security (DHS), Federal Communications Commission (FCC), and the Department of the Treasury to discuss their efforts and authorities to address potential Internet congestion. We also interviewed representatives from telecommunications and Internet providers that are members of the U.S. Communications Sector Coordinating Council that provides input to DHS regarding critical infrastructure protection issues. We also interviewed staff at the Department of Health and Human Services (HHS)—including staff from the Centers for Disease Control and Prevention—to learn about their efforts to educate the public about pandemic strategies. To assess the potential Internet congestion that could occur during a pandemic, we conducted a literature search and reviewed relevant studies and reports. Specifically, we reviewed a study conducted by DHS in cooperation with various government, communication sector, and financial sector representatives.[1] The study evaluated the technical feasibility of the pandemic strategy advocated by the government and identified action plans to better prepare the nation for telecommuting during a pandemic influenza. Our review of the study included an evaluation of the study's methodology, and interviews with the DHS staff who oversaw the research on this study, including the Director and Chief of Staff of the Office of Cyber Security and Communications. To confirm the accuracy of the study's findings, we interviewed communication sector representatives who participated in the study. We also reviewed after action reports from two pandemic exercises—one sponsored by the Financial Services Sector

[1]Department of Homeland Security, *Pandemic Influenza Impact on Communications Networks Study* (Washington, D.C., December 2007).

Coordinating Council, Financial and Banking Information Infrastructure Committee, and the Securities Industry and Financial Markets Association, and another conducted by the United Kingdom financial sector to test the financial sectors' resilience to pandemic influenza.

To assess the actions that critical securities market organizations and key market participants are taking to prepare pandemic plans, we reviewed the actions of seven organizations—including exchanges, clearing organizations, and payment processors—whose ability to operate is critical to the overall functioning of the financial markets. To maintain the security and the confidentiality of their proprietary information, we agreed with these organizations that our report would not discuss their efforts to address pandemic readiness and ensure business continuity in a way that could identify them. To assess how these organizations ensure they can continue operations in the face of a pandemic outbreak, we discussed their business continuity and pandemic preparedness plans with their staff and visited their facilities. We reviewed and analyzed their pandemic plans and supporting business continuity documents and compared the plans to the key elements that banking and securities regulators have issued as guidance to financial organizations regarding pandemic planning. In evaluating these organizations' pandemic readiness, we attempted to determine whether these organizations' pandemic plans adequately address the five elements required by the regulators, including: (1) a process for monitoring the pandemic's progress and a plan that escalates response steps as various pandemic phases are reached; (2) a preventive program to minimize, to the extent possible, illness among employees, including social distancing of employees by curtailing meetings; (3) a documented strategy of facilities or procedures designed to allow the organization to continue its critical operations in the event that large numbers of its staff are unavailable for prolonged periods, including an analysis of staffing levels needed for critical functions and, as applicable, an alternative to teleworking; (4) a testing program to ensure that the practices and capabilities will be effective and allow it to continue its critical operations; and (5) an oversight program to ensure ongoing review and updates to the pandemic plan.

To assess financial regulators' efforts to assess the readiness of securities market organizations to continue operating during a pandemic, we reviewed relevant regulations and guidance and interviewed officials at the Securities and Exchange Commission (SEC), the Board of Governors of the Federal Reserve System (Federal Reserve), and the New York Federal Reserve Bank, the Office of Comptroller of the Currency, and the Financial Industry Regulatory Authority (FINRA). We also collected and

reviewed data and reports from SEC, FINRA, and the Federal Reserve on the examinations they conducted of exchanges, clearing organizations, and broker-dealers. Furthermore, we reviewed a random sample of exams conducted by FINRA of business continuity practices at clearing firms that provide order routing and post-trade clearance and settlement processing for other broker-dealers (introducing firms) from 2006 through 2008. We randomly selected 9 firms of varying sizes from a total population of 56. To assess whether the level of preparations varied by firm size, we reviewed examinations for 3 large firms (that provided clearing for 100 or more other broker-dealer firms), 3 medium-sized firms (those that cleared for between 20 and 99 firms), and 3 small firms (those clearing for 19 or fewer firms). We also interviewed officials at one of the larger clearing firms.

We conducted this performance audit from June 2008 to October 2009 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: FINRA Efforts to Oversee Pandemic Readiness of Broker-Dealers

Although the Financial Industry Regulatory Authority (FINRA)—the self-regulatory organization that oversees most broker-dealers in the United States—undertook some actions to improve broker-dealers' awareness of the potential impact of a pandemic, it has only recently begun to take steps to more fully ensure such firms are making adequate preparations. In addition to oversight by the Securities and Exchange Commission (SEC), FINRA oversees broker-dealers conducting business domestically in the United States. The broker-dealers that FINRA oversees include, but are not limited to, two different types:

- *Introducing* broker-dealer firms whose staff open customer accounts and accept orders to buy and sell securities, but whose firms are not usually members of the exchanges or clearing organizations.

- *Clearing firms* that maintain accounts at the central securities clearing organization and process trades on behalf of their own customers as well as those for the customers of the introducing brokers that use them for trade execution or clearing processing. Clearing firms also maintain the cash and securities holdings for their introducing firms' customers.

According to data from FINRA, as of June 2009, 56 firms that clear for other broker-dealers (clearing firms) were operating in the U.S. markets, with some clearing for hundreds of firms but many clearing for less than 20 firms.[1]

Although most broker-dealers are not required to recommence operations after disasters, FINRA expects its member firms to have business continuity plans that, among other things, assess how pandemic risks could affect the firm. Unlike the core exchanges and clearing organizations and critical broker-dealers covered by the *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*, which SEC requires to be able to resume operations on the same business day on which a wide-scale disruption occurs, broker-dealers have the option of recommencing their operations or shutting

[1]In addition to the 56 firms that clear for other broker-dealers, according to FINRA there are 149 firms that are "self-clearing," meaning they clear transactions, but exclusively for themselves or their customers.

down if they are unable to continue.[2] Since 2004, FINRA has had rules that require broker-dealers to have a business continuity plan in place that describes how the firm will: maintain appropriate backup and recovery functions for critical data; alternate communications between the member and the employees; and maintain all mission critical systems, such as those that process taking orders, and clearing and settling securities trades.[3] As a result, at a minimum the FINRA business continuity rule requires all of its member broker-dealers to have adequate plans for ensuring customers have prompt access to their funds and securities in the event that the broker-dealer discontinues business operations.[4] Although FINRA's business continuity rules were issued before a pandemic was widely recognized as a potential threat to the financial markets, the organization issued guidance in 2006 that encourages broker-dealers to ensure that they assess whether or not their business continuity plans would be suitable for prolonged, widespread public health emergencies, such as a pandemic outbreak.[5] Also in 2006, FINRA requested comment on potential regulatory relief granted in response to a pandemic.[6] FINRA

[2]Under existing securities laws, most broker-dealers cannot be mandated to continue operations. Instead such decisions would be a business decision by such firms. However, a small number of firms have been designated as significant based on their trading volumes in various product markets. These firms are required to be able to reconstitute those parts of their operations needed to complete clearing and settlement of their transactions in these markets within 4 hours to avoid causing potential systemic problems for the markets as a whole.

[3]These rules were issued by FINRA's predecessor organizations: NASD Rules 3510 (Business Continuity Plans) and 3520 (Emergency Contact Information), and NYSE Rule 446 (Business Continuity and Contingency Plans). FINRA has since established a consolidated rule book, integrating rules from both entities, including those covering business continuity and emergency preparedness. FINRA determined that the NASD Rules 3510 and 3520 and NYSE Rule 446 were duplicative, and as a result, effective November 11, 2008, FINRA deleted NYSE Rule 446 and on August 28, 2009, SEC approved FINRA's recommendation to combine and adopt NASD Rules 3510 and 3520, as amended, as FINRA Rule 4370 in the Consolidated FINRA Rulebook. See Securities Exchange Act Release No. 34-60534, 74 Fed. Reg. 44410 (Aug. 28, 2009).

[4]*See* NASD Notice to Members No. 04-37, "SEC Approves Rules Requiring Members to Create Business Continuity Plans and Provide Emergency Contact Information" (May 2004).

[5]This guidance was issued by FINRA's predecessor organization, NYSE, as NYSE Regulation Information Memo No. 06-30 "Guidance Pertaining to Business Continuity and Contingency Plans Relating to a Potential Pandemic" FINRA (May 2006).

[6]This notice was issued by FINRA's predecessor organization, NASD. NASD Notice to Members No. 06-31 "NASD Requests Comment on Regulatory Relief that Should Be Granted in Response to a Possible Pandemic or Other Major Business Disruption" (June 2006).

officials told us they have also emphasized the importance of addressing pandemic as part of business continuity planning to the broker-dealer staff that attend industry conferences and workshops.

However, prior to June 2009, FINRA had not begun to actively assess the readiness of broker-dealers, including clearing firms. FINRA examines firms on a rotational basis—depending on the risk level and complexity of firms' operations—every 1, 2, or 4 years for compliance with a broad range of regulatory issues, including business continuity planning. According to data submitted to us by FINRA, across the 56 firms that clear for other broker-dealers, their staff conducted 40 examinations for compliance with the business continuity rules in 2006, 39 in 2007, 46 in 2008, with 33 completed or scheduled for 2009. When FINRA conducts the business continuity examinations, the inspectors use 1 or more of 13 business continuity planning examination modules to guide the inspection. However, the initial set of business continuity examination modules that FINRA staff have been using in their examinations to assess firms' compliance with the business continuity rule did not include questions related to pandemic preparedness.

In addition, our own review of FINRA-conducted inspections found that FINRA officials have not been addressing pandemic issues to a great extent in business continuity examinations conducted through June 2009. We reviewed FINRA business continuity exams from 2006 to 2008 for a randomly selected sample of 9 of the 56 clearing firms that clear for other firms to assess the extent to which pandemic issues were being addressed. To assess whether the level of preparations varied by firm size, we reviewed examinations for 3 large firms (that provided clearing for 100 or more introducing brokers), 3 medium-sized firms (those that cleared for between 20 and 99 firms), and 3 small firms (those clearing for 19 or fewer firms). Our review found that the inspections for 8 of the 9 firms showed evidence the FINRA examiner reviewed the firm's plan for compliance with the 10 business continuity elements required to be addressed by FINRA's business continuity rule. However, we found limited evidence that the examiners reviewed pandemic readiness at the firms. For three of the firms, the examination documentation included some general discussions about these firms' pandemic planning, and in three cases we saw evidence that pandemic plans were included in the documents reviewed by the FINRA examiners.

Although the full extent to which clearing firms are ready to continue operating during a pandemic has not been assessed, some evidence raised concerns that not all are making adequate preparations. We did not

attempt to systematically determine clearing firms' pandemic readiness, but we did interview staff at one of the largest clearing firms. This firm's staff described a pandemic plan and procedures that appeared reasonably likely to be able to continue operations even in the face of significant absenteeism. However, as noted earlier, a limited review by SEC staff conducted in 2008 found that three of four midsized clearing firms have not developed plans for continuing operations during a pandemic. If clearing firms such as these are not able to continue operating, customers of the introducing broker-dealers that use the clearing firms experiencing such problems potentially could find access to their funds and securities curtailed for significant periods of time. For example, FINRA staff told us transferring the customer accounts of broker-dealers that cease operations can take several days or weeks, depending on the circumstances.

In response to the recent H1N1 outbreak and our inquiries in relation to this review, FINRA staff told us they have begun various efforts to more broadly assess the readiness of broker-dealers, including clearing firms, for a pandemic. Beginning in June 2009, FINRA conducted a voluntary survey of broker-dealer firms to determine preparedness for a pandemic. The survey included questions asking, among other things, whether the firm has conducted a review of the potential impact of a pandemic, and whether the firm has a business continuity plan specifically addressing a pandemic, and if so, how that plan is being tested. The survey results show that almost all respondents report having conducted a review of the potential impact of a pandemic, and have business continuity plans that specifically address pandemic preparedness. FINRA is using the results of the survey to develop additional guidance on pandemic preparedness practices for the industry. In addition, FINRA staff told us they have developed a new examination module that addresses pandemic preparedness. This module requires their examiners to determine whether the firm's business continuity arrangements for resuming business operations appear reasonable given the conditions likely to prevail during a pandemic. For example, the module directs the examiner to review the firm's business continuity planning to determine if the procedures address risks associated with pandemic, such as taking steps to limit the spread of influenza among its staff, and assessing the firm's operational capabilities using teleworking and the impact of requiring employees to work remotely. The new module was piloted by FINRA examiners during the summer of 2009, and then, once revised as needed, will be used in upcoming exams. FINRA officials told us they will conduct a pandemic preparedness review at all the firms that clear for other broker-dealers by the end of 2011.

Appendix III: Steps Taken by Bank Regulators to Assess Pandemic Preparedness in Key Clearing Banks

Banking regulators for the key clearing banks have taken actions to assess pandemic readiness among banks, including those that clear transactions for the securities markets. The Federal Reserve and the Office of Comptroller of the Currency issued guidance in 2006 that call for all banks under their supervision to include the unique impacts of a pandemic in their business continuity planning.[1] Similar to securities regulators, the bank regulators had taken actions to help banks and thrifts address pandemic efforts in our last review. For example, in a joint notice from the regulators that oversee banks and thrifts, the agencies indicated that their institutions should review the U.S. government's national pandemic strategy to consider what actions may be appropriate for their particular situations, and whether such actions should be included in their event response and contingency strategies.[2] Furthermore, banking regulators had also begun to review pandemic planning in the context of their ongoing supervisory activities. However, in response to the recommendation we made in our 2007 report, the Federal Reserve and the Office of the Comptroller of the Currency subsequently notified institutions that play systemically important roles in securities and other markets that these entities should have plans that address even severe pandemics. In addition, the Federal Financial Institutions Examination Council issued an updated examination manual regarding information technology and business continuity issues that includes steps that banks should be taking related to pandemic planning.[3]

Banking regulators have also been conducting reviews to ensure that banks are preparing for possible pandemics, and through these efforts confirmed that the critical market institutions under their supervision met the 2007 deadline to have a pandemic plan in place, and that those plans include the required elements. For example, the Federal Reserve began a

[1]This report is concerned with clearing banks—those institutions that clear trading transactions for the markets. Therefore we do not discuss other banking regulators, such as the Federal Depository Insurance Corporation, or state banking regulators.

[2]*Interagency Statement on Pandemic Planning* (Dec. 18, 2007).

[3]Federal Financial Institutions Examination Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, and to make recommendations to promote uniformity in the supervision of financial institutions. FFIEC IT Examination Handbook, *Business Continuity Planning, BCP* (March 2008).

series of reviews—using a set of questionnaires to collect information on the planning elements established in the guidance—in January 2008 to assess the progress made by the top 15 banking organizations in the country and concluded that considerable progress has been made among its member banks in pandemic planning. The review objectives were to provide a broad perspective of the state of pandemic preparedness at systemic institutions, identifying trends within the pandemic preparedness planning process, and to provide peer benchmarking attributes to the participating institutions. Office of the Comptroller of the Currency officials told us they continue to monitor progress on pandemic planning in national banks through ongoing supervision rather than targeted exams, and they have been evaluating the banks' efforts using the newly issued business continuity planning guidance that includes the requirements for pandemic plans.

Appendix IV: Comments from the Securities and Exchange Commission

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

THE CHAIRMAN

September 23, 2009

Mr. Mathew J. Scire
Director, Financial Markets and Community Investment
United States Government Accountability Office
441 G St., NW
Washington, DC 20548

Dear Mr. Scire:

This letter responds to your request, dated September 10, 2009, to review and comment on the draft Report entitled Pandemic Preparedness: Key Securities Market Participants Are Making Progress, but Agencies Could Do More to Address Potential Internet Congestion and Encourage Readiness (GAO-10-08).

Thank you for the opportunity to comment on the draft GAO Report. We appreciate the Report's acknowledgement that significant progress has been made by critical securities market organizations to continue operations during a pandemic or other wide-scale disruption. In particular, the Report recognizes that critical market organizations have devoted considerable resources since September 11, 2001, to: (1) develop and maintain proprietary communications networks independent of the public telecommunications networks and the Internet; (2) establish geographically diverse backup sites to maintain critical functions during a wide-scale disruption, including a pandemic; (3) expand their existing business continuity plans to address the pandemic threat; and (4) test their plans during an extensive industry-wide pandemic exercise in late 2007.

While the key securities exchanges and clearing organizations use proprietary networks that bypass the Internet, nevertheless we share the GAO's concern that Internet congestion could significantly impair some aspects of the securities markets during a pandemic. Internet congestion could severely impair the ability of investors and market professionals to access current market data and place orders. We therefore agree with GAO that more needs to be done to address potential Internet congestion, and we are prepared to continue to assist the appropriate agencies to address this problem.

In addition, we agree with GAO that critical market organizations can do more to make their existing pandemic plans even better. Accordingly, the Commission staff plans to issue letters to critical market organizations recommending that they further document their staff cross-training arrangements and their plans to maintain operations if Internet congestion impairs their ability to rely on telework for support functions. Further, we will incorporate a review of their compliance with this recommendation in our future examinations of these organizations.

Mr. Mathew J. Scire
Page 2

Thank you again for the consideration that you and your staff have shown to our staff and the opportunity to comment on this draft Report. If it would be useful to elaborate on the discussion in this letter, please contact Jamie Brigagliano, Co-Acting Director, Division of Trading and Markets, at (202) 551-5700, or John Walsh, Acting Director, Office of Compliance Inspections and Examinations, at (202) 551-6471.

Sincerely,

Mary L. Schapiro
Chairman

Appendix V: Comments from the Department of Homeland Security

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

October 14, 2009

Mathew J. Scire
Director
Financial Markets and Community Investment
Center for Technology and Engineering
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Scire:

Re: GAO 10-08, *Key Securities Market Participants Are Making Progress, but Agencies Could Do More to Address Potential Internet Congestion and Encourage Readiness*

The Department of Homeland Security (DHS) appreciates the opportunity to review and comment on the U.S. Government Accountability Office's (GAO) draft report referenced above. The GAO came to several conclusions with regard to the current state of Internet congestion and readiness. The Department recognizes the nature of Internet congestion and will continue working with Federal and industry stakeholders to solicit and share best practices.

DHS is responsible for specific national security/emergency preparedness (NS/EP) communication functions and mission, which include planning for, developing, and implementing enhancements to the national telecommunications infrastructure to achieve measurable improvements in survivability, interoperability, and operational effectiveness under all conditions and seeking greater effectiveness in managing and using national telecommunication resources to support the Federal Government during any emergency. The Department agrees that strong cooperation between the private and public sectors is essential to support those functions, which among others, is the responsibility of the National Coordinating Center (NCC).

The NCC leverages its unique joint government/industry structure and all-hazard emergency response capabilities to coordinate the initiation, restoration, and reconstitution of Federal Government national security and emergency preparedness telecommunications services both nationally and internationally. Internet congestion, as a general matter and with regard to non-NS/EP communications, does not fall within the Department's responsibilities. The Department believes GAO's recommended actions fall within the operational and administrative interest of other Federal Agencies. Therefore, the Department concurs with GAO's recommendations that the Secretary should do the following, insofar as they relate to the maintenance of nationally critical communications, that is, NS/EP communications:

(1) Develop a strategy outlining actions that could be taken to address potential Internet congestion;
(2) Coordinate with other relevant federal and private sector entities about actions that could potentially reduce Internet congestion;
(3) Work with other federal partners to determine if sufficient authority exists for one or more relevant agencies to take any contemplated actions to address Internet congestion; and
(4) Assess the effectiveness and feasibility, and undertake if warranted, a public education campaign to reduce such congestion.

With regard to implementing these recommendations for NS/EP communications, the Department is currently working to enhance its programs to assure NS/EP communications under all conditions, including a pandemic. Additionally, under the National Response Framework, the Department will continue to work with departments and agencies in support of Emergency Support Function #2 (ESF#2) - Communications, specifically, to support the restoration of the communications infrastructure, facilitate recovery from cyber attacks, and coordinate Federal efforts during incidents requiring a coordinated federal response.

General Comments:

- DHS is not responsible for addressing Internet congestion caused by an increase in high-bandwidth Internet applications and services, or increased use over time that eventually exceeds the Internet service providers' capacity. These latter examples are real-world concerns, but, absent an adverse effect on NS/EP communications, they are not within DHS' general purview to address.

- DHS' responsibility for NS/EP does not include managing the Internet during a pandemic; moreover, DHS does not have the responsibility for developing an Internet Congestion strategy separate and apart from assuring NS/EP communications. DHS agrees that its strategy for assuring NS/EP communications should include addressing the possible consequences of a pandemic.

- The report gives the impression that there is potentially a single solution to Internet congestion that DHS could achieve if it were to develop an appropriate strategy. All users which rely on the Internet, including the financial services sector, should not expect that Internet congestion problems will be easily solved, and should develop pandemic continuity of operations plans that do not rely on unimpeded Internet access. An expectation of unlimited Internet access during a pandemic is not realistic, any more so than an expectation that traffic congestion on hurricane evacuation routes can be completely avoided. This is not to say that DHS has not taken steps to share best practices and explore other options for reducing congestion during a pandemic or a hurricane. But users should base their own plans and activities on realistic expectations, rather than assuming that anticipated congestion problems can be readily addressed.

- 3 -

See comment 1.

- **Page: 14**

Issue: *Furthermore, the government has recommended teleworking as an option for businesses to keep their operations running during a pandemic. Thus, many workers will be performing their work from home and will be competing with recreational and other users for band width.*

DHS Response: Recommending that individuals telework (in extremis situations) is appropriate. Government, industries, and citizens have the responsibility for planning and implementing necessary actions prior to or during an event, and telework is an appropriate option to be considered. In this regard, Internet congestion is analogous to the telephone congestion that individuals experience during high volume days (e.g., day after Thanksgiving). In these situations, communications providers have mechanisms to reduce congestion to maintain agreed-upon service levels as well as other contractual obligations. Similarly, although pandemic-related congestion could last longer, and the Internet falls under a different set of policy restrictions than the telephone network, it is important that communications providers develop plans, considering best practices developed by industry and/or suggested by government, for maintaining service. And government must continue to develop plans and implement programs to assure the availability of NS/EP communications under all conditions, including pandemic, which is an ongoing program of work for the NCS.

See comment 2.

- **Page: 17**

Issue: *A 2007 DHS Study that was conducted in cooperation with various government, communications sector, and financial sector entities used modeling of residential and other network configurations to confirm that the increased traffic generated in neighborhoods during a pandemic is likely to exceed the capacity of the providers' aggregation devices in metropolitan residential neighborhoods.*

DHS Response: The study did not include the effect of network management (FCC Memorandum Opinion and Order FCC 08-183 network management options) on reducing Internet congestion. Internet network management techniques are available to Internet providers. The study only states, "Remote network management tools may be important for network service providers to continue to operate with a reduced workforce."

See comment 3.

- **Page: 24**

Issue: *For example the guidelines for information technology and communications sectors recommend that entities in these sectors consider advising employees to limit household use of streaming video or other bandwidth-intensive Internet activities.*

DHS Response: While this statement is correct, the guidelines and recommendations may or may not correct Internet congestion, depending on citizens' compliance.

DHS suggests the following be added to clarify for accuracy:

- 4 -

FCC Opinion and Order FCC 08-183 indicates that there are several methods available that an Internet provider can use for network management. Paragraph 49 indicates that "Comcast could throttle back the connection speeds of high capacity users (rather than any user who relies on peer-to-peer technology, no matter how infrequently). Or Comcast can work with the application vendors themselves. . . ."

- **Page: 24**

See comment 4.

Issue: *Because the practices suggested in these documents sometimes discussed proprietary information, they were only made available to sector council members.*

DHS Response: The Alliance for Telecommunications Industry Solutions' (ATIS) Network Reliability Steering Committee (NRSC) recently released a set of Pandemic Planning recommendations. This document includes a compilation of existing – as well as newly-developed – industry consensus best practices to ensure service provisioning and business continuity in the event of a pandemic outbreak. The guidance includes 56 voluntary best practices that continue the U.S. communications industry's nearly 20-year history of collaboration among experts to promote the health of the nation's public networks. The Best Practices are available at: http://www.atis.org/nrsc/Docs/NRSC_Pandemic_Checklist_Final.pdf.

- **Page: 27**

See comment 5.

Issue: *Finally, one financial sector organization noted that the plan should include a prioritization scheme to prioritize Internet traffic based on how critical it is to national and economic security.*

DHS Response: The report should note that FCC principles might impede such prioritization, depending upon their scope and application. See FCC Policy Statement FCC 05-151, which states, "As a result, the Commission has jurisdiction necessary to ensure that providers of telecommunications for Internet access or Internet Protocol-enabled (IP-enabled) services are operated in a neutral manner."

- **Page: 28**

See comment 6.

Issue: *Although its own study identified voluntary public reduction of Internet use as an effective means of reducing pandemic congestion, DHS has not begun steps to assess the feasibility and effectiveness of obtaining such public cooperation.*

DHS Response: The Office of the Manager, National Communications System (OMNCS) actively promotes the issuance of consumer practices through industry providers. Specifically, ATIS (see general comment #10) released best practices. In such cases, industry provides recommendations to its customers and can follow up with public service announcements advising consumers of recommended activities. Such activities help to mitigate the risks from events such as a pandemic.

See comment 7.

- **Page: 29**

  Issue: *However, DHS staff told us they had not begun efforts to evaluate the feasibility or effectiveness of such a campaign or taken steps to begin developing such an effort because of the demands of other crises.*

  DHS Response: This mischaracterizes the Department's previously stated position. The Department's position is that there are activities supporting our operational mission that must take priority over a public service campaign on this topic. Please also refer to the second and third general comments above.

See comment 8.

- **Pages: 33-34**

  Issue: *Although congestion during a pandemic could interfere with individuals' ability, including teleworkers and others, to access the Internet, the primary communications of the critical market organizations would not be affected because these organizations and their participants communication via high-capacity, proprietary networks that do not traverse the public Internet infrastructure.*

  DHS Response: The report does not explain to what extent congestion of the public Internet infrastructure would affect the financial services sector. Moreover, the report does not discuss the contractual obligations that are in place between the service provider and its customers. The report should address this issue. Pages 39-41 partially address this issue, saying that firms are assessing their work-from-home capabilities, but the report does not describe the results of this assessment.

We appreciate the opportunity to review and comment on this draft report and we look forward to working with you on future homeland security issues.

Sincerely,

Jerald E. Levine
Director
Departmental GAO/OIG Liaison Office

The following are GAO's comments on the Department of Homeland Security's letter dated October 14, 2009.

GAO Comments

1. The likely usefulness of teleworking as a way for government agencies and businesses to continue operations during a pandemic is one of the reasons we believe that DHS should take the lead in addressing potential Internet congestion that could arise during a severe pandemic, including working with private sector providers to encourage them to take proper steps to be prepared not only to ensure that NS/EP communications are not affected, but that any adverse impact on all other communications is also mitigated.

2. Although not citing the FCC opinion and order by number, our report does discuss some of the network management techniques noted by those documents that providers might be able to use to relieve pandemic-related congestion. However, as our report notes, these techniques may have limitations in resolving the type of congestion envisioned to occur in residential neighborhoods. In addition, providers told us that they would require government direction to implement such techniques to reduce congestion, which is why we recommend that DHS begin taking steps to determine what strategies, actions, and authorities are needed to address this issue so that if it appears that private sector providers must be asked to take steps, such direction can come from the appropriate government source.

   Furthermore, as the report notes, providers told us their remote network management tools may be a way for them to continue their operations with reduced workforces resulting from pandemic-related absenteeism and that these tools could be used to re-route traffic around congested areas in regional networks or the national backbone, but not to relieve congestion in the residential neighborhoods.

3. As our report states, the DHS study of the impact of pandemic on Internet access notes that obtaining the cooperation of the general public in limiting bandwidth-intensive Internet activities was shown by the study's modeling to be an effective way to relieve congestion. Uncertainty over whether such cooperation could be obtained is the reason that we recommend that DHS assess the effectiveness and feasibility of implementing a public information campaign, and if warranted, begin developing one. Regarding DHS's suggested addition of the techniques noted in the FCC order, as we noted above, we discussed these techniques with providers and learned they may have limitations in addressing the type of congestion envisioned to arise in a

pandemic and providers would likely require government direction to take such actions.

4. This comment was sent to us earlier as a part of DHS's technical comments and we have revised the text to note that some of this information has been made available publicly. The best practices that DHS cites in response would likely improve telecommunication providers' readiness for a pandemic, but likely would not be sufficient to relieve the congestion in residential neighborhoods.

5. This statement was intended to serve as an example of the types of comments FCC received regarding the prioritization issue. We did not assess whether this suggestion was feasible or comports with other FCC practices.

6. As noted above, the best practices DHS cites could assist providers in being better prepared for a pandemic. However, they are not likely sufficient to address residential neighborhood congestion, which is why DHS's own study also proposed best practices for enterprises, teleworkers, and the public. Providers did not provide us information on any steps they were taking to advise the public about practices that could relieve congestion during a pandemic. In fact, one provider told us a good approach to manage Internet congestion effectively would be for the government to work with providers to publicize appropriate best practices and issue related guidance. As a result, we recommend that DHS assess the effectiveness and feasibility of such practices and implement such a campaign if warranted.

7. We changed the language in this report to note that DHS has not taken action related to evaluating a public education campaign because other activities supporting its operational mission have taken priority. Nevertheless, we believe that such activities should be undertaken to address potential pandemic-related congestion.

8. As this report discusses, much of the securities market's critical communication would not be affected by congestion of the public Internet infrastructure because it travels over dedicated proprietary networks. However, financial sector organizations are planning to use teleworking to varying degrees as part of their plans to continue operations during a pandemic. As a result, these staff, as a well as the staff of other U.S. federal, state, or local governments and private businesses that plan to use teleworking from home during a pandemic would be affected by the congestion that is envisioned to affect

residential neighborhoods. As a result, we recommend that DHS to take actions to address this issue.

Furthermore, our report discusses securities market organizations' activities to prepare themselves to effectively telework during a pandemic and describes the limitations we found in these efforts. As a result, we made recommendations to SEC to further improve its oversight, which it has agreed to implement.

Appendix VI: GAO Contacts and Staff Acknowledgments

GAO Contacts

Mathew J. Scire, (202) 512-8678 or sciremj@gao.gov
David A. Powner, (202) 512-9286 or pownerd@gao.gov
Nabajyoti Barkakati, (202) 512-4499 or barkakatin@gao.gov

Acknowledgments

In addition to the contacts named above, Cody Goebel and Michael Gilmore, Assistant Directors; Chir-Jen Huang; Yola Lewis; Kristeen McLain; Marc Molino; Carl Ramirez; Linda Rego; and Hai Tran made major contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Please Print on Recycled Paper