

GAO

Report to the Chairman, Committee on  
Financial Services, House of  
Representatives

November 2005

# INSURANCE SECTOR PREPAREDNESS

Insurers Appear  
Prepared to Recover  
Critical Operations  
Following Potential  
Terrorist Attacks, but  
Some Issues Warrant  
Further Review





Highlights of [GAO-06-85](#), a report to the Chairman, Committee on Financial Services, House of Representatives

## Why GAO Did This Study

The insurance sector is a key part of the U.S. financial sector, particularly following a terrorist attack or other disaster where there has been loss of life and damage to property. To determine the insurance sector's preparedness to protect and recover critical insurance operations, GAO was asked to (1) describe the potential effects of disruptions to the operations of insurers, state insurance regulators, and the National Association of Insurance Commissioners (NAIC); (2) identify actions taken by those organizations to protect and restore their operations; and (3) assess the extent to which regulations require reviews of insurer efforts in these areas.

## What GAO Recommends

GAO recommends that state regulators, working through NAIC and appropriate state officials, ensure that state insurance regulators implement appropriate capabilities for recovering critical functions following a disruption. GAO also recommends that NAIC act on its decision to have more frequent independent testing of its information security environment. Finally, GAO recommends that state regulators, as they review the adequacy of their examination processes, consider whether changes are needed to examination content and structure related to business continuity, recovery time objectives, and outsourcing.

[www.gao.gov/cgi-bin/getrpt?GAO-06-85](http://www.gao.gov/cgi-bin/getrpt?GAO-06-85).

To view the full product, including the scope and methodology, click on the link above. For more information, contact Orice M. Williams at (202) 512-8678 or [williamso@gao.gov](mailto:williamso@gao.gov).

# INSURANCE SECTOR PREPAREDNESS

## Insurers Appear Prepared to Recover Critical Operations Following Potential Terrorist Attacks, but Some Issues Warrant Further Review

### What GAO Found

Adequate business continuity capabilities are necessary to prevent terrorist attacks or natural disasters from severely disrupting the operations of large insurers and leaving the companies unable to provide important services to policyholders when needed. And while a disruption to a large insurer could potentially affect millions of policyholders, any effects would likely not spread throughout the insurance sector because of limited interdependencies among insurers and, unlike the securities markets, the lack of a single point through which insurance transactions must pass. Further, while state insurance regulators and NAIC provide important services to consumers and insurers, such services are generally not time sensitive and a disruption of 1 or 2 weeks would not have a significant effect.

All of the 18 insurers and most of the five state regulators GAO spoke with, as well as NAIC, indicated that they had taken actions designed to protect their operations from disruption and recover critical operations should a disruption occur. For insurers, these actions typically included establishing geographically dispersed backup sites and conducting critical operations at multiple geographically dispersed facilities. Among property/casualty and life insurers, the highest priority was generally to recover investment and cash management functions, while among health insurers it was customer service and claims processing. Most insurers said they could recover their highest priority operations within 1 day, and most other operations within 3 days. While all of the state regulators GAO spoke with had processes in place to back up critical data, one had no backup computer systems, one had no business continuity plans, and one had neither. NAIC has also taken steps to protect critical data and has implemented business continuity capabilities designed to recover critical operations within 24 hours.

Current federal and state regulations, as well as NAIC examination guidelines, require insurers to have information security programs and business continuity plans, but do not require minimum recovery times. For example, state insurance examinations review information security and business continuity as part of the larger objective of reviewing insurers' internal controls and insurer solvency, and do not require insurers to meet specific recovery objectives. However, while state regulators stated they had informal expectations that insurers would recover certain critical operations, such as claims processing, within 2 days after a disruption, half of the insurers GAO spoke with had set recovery goals for their claims processing operations that would appear not to meet these expectations. Further, it is not clear whether current examination guidelines and practices adequately address the trend among insurers to outsource certain functions, especially information technology functions. For example, some of the insurers GAO spoke with were outsourcing their computer system backup functions or portions of their claims-processing operations, but only one of the regulators said they had ever conducted audit work at such a service provider.

---

# Contents

---

---

## Letter

Results in Brief	1
Background	2
Disruptions to Insurers' Operations Could Delay Services to Policyholders, but Disruptions at State Regulators or NAIC Would Have Limited Short-Term Effects	5
Insurers, Most State Regulators, and NAIC Have Taken Actions Designed to Protect and Recover Their Critical Operations	8
Current Laws and Regulations and State Insurance Examinations Require Insurers to Have Business Continuity and Information Security Plans but Generally Do Not Set Minimum Capabilities	11
Conclusions	23
Recommendations for Executive Action	27
NAIC Comments and Our Evaluation	28
	29

---

## Appendixes

<b>Appendix I: Objectives, Scope, and Methodology</b>	31
<b>Appendix II: Comments from the National Association of Insurance Commissioners</b>	34
<b>Appendix III: GAO Contact and Staff Acknowledgments</b>	37

---

## Figures

Figure 1: Insurer's Mobile Operations Vehicle	15
Figure 2: Insurer Recovery Time Objectives for Several Insurer Functions	16

---

**Abbreviations**

9/11	September 11, 2001, terrorist attacks
DHS	Department of Homeland Security
FBIIC	Financial and Banking Information Infrastructure Committee
FEMA	Federal Emergency Management Agency
FFIEC	Federal Financial Institutions Examination Council
FISCAM	Federal Information Systems Control Audit Manual
FSSCC	Financial Services Sector Coordinating Council
GLBA	Gramm-Leach-Bliley Act
HIPAA	Health Insurance Portability and Accountability Act of 1996
ISQ	Information Systems Questionnaire
NAIC	National Association of Insurance Commissioners
SAS	Statement on Auditing Standards
Treasury	Department of the Treasury

This is a work of the U.S. government and is not subject to copyright protection in the United States. It 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.



United States Government Accountability Office  
Washington, D.C. 20548

November 18, 2005

The Honorable Michael G. Oxley  
Chairman  
Committee on Financial Services  
House of Representatives

Dear Mr. Chairman:

As you know, the insurance sector is a key component of the U.S. financial sector and is vital to the overall functioning of our nation's economy, particularly following a terrorist attack or other disaster, such as a hurricane, in which lives have been lost, property has been damaged, and people and businesses need funds to rebuild their lives. The smooth functioning of the insurance sector depends on the ability of key businesses and organizations to protect their operations from disruption and recover their operating ability quickly should a disruption occur. The importance of such preparedness was made clear when, in August 2004, the Department of Homeland Security (DHS) announced that terrorists had identified several financial institutions as potential targets, including at least one large insurer.

GAO has previously reviewed the actions taken by critical financial market participants to ensure the continued processing of securities transactions and to reduce the potential for disruptions to market operations after disasters such as the September 11, 2001, terrorist attacks (9/11).<sup>1</sup> Your request that we perform similar work with respect to the insurance sector is in many ways an extension of this earlier work. As agreed with the committee, our objectives for this project were to

- describe the potential effects of disruptions to the operations of insurers, state insurance regulators, and the National Association of Insurance Commissioners (NAIC);<sup>2</sup>

<sup>1</sup>See GAO, *Financial Market Preparedness: Improvements Made, but More Action Needed to Prepare for Wide-Scale Disasters*, [GAO-04-984](#) (Washington, D.C.: Sept. 27, 2004); *Potential Terrorist Attacks: Additional Actions Needed to Better Prepare Critical Financial Market Participants*, [GAO-03-251](#) (Washington, D.C.: Feb. 12, 2003); and *Potential Terrorist Attacks: Additional Actions Needed to Better Prepare Critical Financial Market Participants*, [GAO-03-414](#) (Washington, D.C.: Feb. 12, 2003).

<sup>2</sup>NAIC is a voluntary organization of the chief insurance regulatory officials of the 50 states, the District of Columbia, and four U.S. territories.

- 
- identify the actions these organizations have undertaken to protect their operations from disruption and restore operations should a disruption occur; and
  - assess the extent to which certain current laws and regulations require reviews of insurers' efforts in these areas and the extent to which state examinations include such reviews.

To achieve our objectives, we reviewed regulatory documents, such as insurance laws and examination guidelines, and interviewed officials from a judgmental sample of 18 large health, life, and property/casualty insurers in five states, the insurance regulators in those states, and NAIC regarding their business continuity capabilities and their physical and information security protections. The insurers were selected, in part, based on total revenue in 2003 and included 5 health insurers, 6 life insurers, and 7 property/casualty insurers. In assessing the organizations' capabilities in these areas, we used criteria that were either established by regulators or were generally accepted by government or industry. For our reviews, we generally relied on documentation and descriptions provided by the organizations, although we did directly observe some security controls and business continuity elements at NAIC and at some insurers. As part of our work to assess actions taken by state insurance regulators, we also reviewed a sample of examination workpapers from each of the state regulators we contacted. We performed our work from December 2004 through October 2005 in accordance with generally accepted government auditing standards. For security reasons, we have not included in this report the names of the insurers and state insurance regulators we spoke with or their locations.

---

## Results in Brief

Adequate business continuity capabilities are necessary to ensure that natural disasters or terrorist attacks do not severely disrupt the operations of large insurers and leave the companies unable to provide important services that policyholders need at such times. These services—all of which could be delayed by a major disruption—include assessing damage, processing and paying claims, providing annuity payments, and ensuring access to medical care. However, we found that several characteristics of the insurance sector would likely restrict the potential effects of a disruption at one insurance firm to that insurer's policyholders and mitigate the potential effects on the larger insurance sector. First, limited interdependencies exist among insurers, so that a disruption at one insurer would not negatively affect other insurers. Second, unlike the securities

---

markets, the insurance market has no single point through which insurance transactions must pass. And third, insurance markets are not geographically concentrated. Insurers also told us that previous potentially disruptive events—such as 9/11, power outages, and hurricanes—had not caused any significant disruptions to their operations. Further, we found that disruptions at state insurance regulators or NAIC would, in the short term, generally have limited effects on policyholders and the insurance industry. State insurance regulators also provide services to consumers—for example, resolving complaints—as well as to insurers, for which they license agents, conduct examinations, and approve insurance rates and products. But these services did not appear to be highly time sensitive, and a delay of even 1 or 2 weeks would not be significant. NAIC primarily provides services to state regulators, including such tasks as analyzing insurers' financial data, and insurers, for which it operates systems that automate licensing for agents and facilitate the processing of requests for insurance product and rate approvals. As with state regulators, while a disruption to the operations of NAIC could potentially delay the provision of these services, such services are not considered highly time sensitive. In addition, manual or other processes exist that regulators and insurers could use in place of nonfunctioning automated systems, although these processes would not be as fast or efficient.

All 18 of the insurers and most of the state regulators we spoke with, as well as NAIC, indicated that they had taken actions designed to protect their operations from disruption and allow for the recovery of critical operations following a disruption. For the insurers, actions to protect their operations included physical security measures such as employee access badges and security guards to prevent unauthorized access to their facilities, and information security measures such as password controls and firewalls to prevent unauthorized access to their computer systems. Actions to ensure recovery of critical operations typically included establishing geographically dispersed backup sites and conducting critical operations at multiple geographically dispersed facilities. Among property/casualty and life insurers, the highest priority was generally to recover investment and cash management functions, while among health insurers it was generally customer service and claims processing. Most insurers told us that they could recover their most critical operations within 1 day and most other operations within 3 days. No insurers had recovery time objectives for any critical systems beyond 5 days. All five state insurance regulators we spoke with had processes in place to back up their critical data, but one had no backup computer systems, one had no business continuity plans, and one had neither. NAIC has taken steps to

---

protect critical data in its possession and has implemented business continuity capabilities designed to recover critical operations within 24 hours. In addition, NAIC officials told us that they can aid state regulators' business continuity efforts by backing up critical regulatory data and providing some resources to state regulators in the event of a disruption.

Certain current federal and state laws and regulations, as well as NAIC examination guidelines, require insurers to have information security programs and business continuity plans but do not require minimum recovery times. For example, insurers must generally comply with laws and regulations that require them to protect consumer data and have internal controls in place, but none of these laws and regulations require insurers to have certain recovery capabilities. Similarly, while NAIC examination guidelines require examiners to determine whether an insurer's business continuity plan is current, covers all critical areas, and has been tested, the guidelines do not require insurers to meet minimum recovery time objectives. Examiners review insurers' business continuity plans as part of the larger objectives of reviewing insurers' internal controls and evaluating insurer solvency. Insurance regulators told us that insurers' ability to service policyholders promptly after a disruption is of concern to them, but current examination guidelines and guidance may not reflect this concern. For example, all five regulators told us that although they generally expected that insurers would be able to recover their claims-processing operations within 2 days, the examination process does not seek to determine whether insurers can meet this expectation. In addition, half of the insurers we spoke with had set goals for recovering their claims-processing operations that would seem to not meet this expectation. Finally, it is not clear whether current examination guidelines and practices adequately address the trend among insurers to outsource certain functions, especially information technology functions. For example, some of the insurers we spoke with were outsourcing their computer system backup functions or portions of their claims-processing operations, but only one regulator had conducted audit work at such a service provider.

Although widespread disruptions to insurers, regulators, and NAIC from a terrorist or natural disaster are less likely to lead to wider disruptions in the financial sector, we are making a number of recommendations aimed at further limiting the potential inconvenience to customers. First, we recommend that state insurance regulators, working through NAIC, take steps to ensure that all state regulators implement consistent, appropriate business continuity capabilities. Second, we recommend that NAIC increase the frequency with which they obtain independent evaluations of



---

their information security controls and overall computer environment vulnerabilities. Finally, we recommend that state insurance regulators, working through NAIC as part of their regular review of the adequacy of state examination guidelines and practices, examine the current placement of the review of insurers' business continuity capabilities within the current examination structure, the need for minimum recovery time objectives for certain insurer services, and the adequacy of current examination guidelines and practices related to the review of insurers' outsourcing of critical functions.

We provided a draft of this report to NAIC for its review and comment. In response, NAIC's Executive Vice President and Chief Executive Officer provided written comments that generally agreed with our findings and recommendations regarding the preparedness of the insurance sector for potential disruptions. NAIC's comments are discussed later in this report and are reprinted in appendix II. NAIC also provided technical comments that were incorporated as appropriate.

---

## Background

Insurers, state insurance regulators, and NAIC all have roles that are key to the continued functioning of the insurance sector and important to U.S. consumers and businesses. Insurers provide services that allow individuals and businesses to manage their risk by providing compensation for certain losses or expenses, such as car crashes, fires, medical services, or loss of the ability to work. Some insurers also provide access to certain financial services, such as annuities and mutual funds. State insurance regulators are responsible for enforcing state insurance regulations, and do so primarily through the licensing of agents, the approval of insurance rates and products, and the examination of insurers' financial solvency and conduct. State regulators typically conduct financial solvency examinations every 3 to 5 years, while examinations reviewing insurers' conduct are generally done in response to specific complaints by consumers or concerns on the part of the regulator. State regulators also monitor the resolution of consumer complaints against insurers.

NAIC is a body composed of state insurance regulators, and while it does not regulate insurers, it does provide optional services designed to make certain interactions between insurers and regulators more efficient. For example, NAIC operates automated systems that insurers can use to request approvals from state regulators for new insurance products and rates as well as licenses for their insurance agents. Most of the insurers and state regulators we spoke with used these services to some extent,

---

although some insurers said that they did not. NAIC also provides services to state regulators that help them monitor insurers' financial condition and prepare for examinations. This service primarily involves collecting financial data that insurers are required by state insurance regulations to provide to NAIC, analyzing that data, and providing the analyses to state regulators. State regulators can also access this database to conduct analyses of their own. According to NAIC, all state regulators use these services to at least some extent. Finally, NAIC develops guidance to be used by state examiners, regularly updating this guidance to ensure it adequately addresses existing or emerging conditions in the insurance sector.

---

### Organizations Take Actions to Protect Operations from Disruption, and Recover Operations Should a Disruption Occur

In order to protect their operations from potential disruptions, organizations can invest in both physical and information security measures. Physical security measures are intended to reduce the risk that facilities and personnel could be harmed by individuals or groups attempting unauthorized entry, sabotage, or other criminal acts. Typical measures might include employee access badges, security guards, or video monitoring systems. Information security measures are intended to protect the confidentiality, integrity, and availability of an organization's information and information systems and to reduce the risk and magnitude of harm resulting from threats such as hackers and computer viruses. These measures might include password controls, firewalls, and intrusion detection systems.

In order to recover their operations should a disruption occur, organizations can develop business continuity plans and invest in business continuity capabilities. Organizations design such plans to guide their response to disruptions, and generally create their plans by identifying the most critical functions and the resources needed to carry out those functions. Business continuity plans and capabilities might include alternate work space should facilities become inaccessible, and backup computer systems and data centers should primary systems and facilities be damaged or destroyed.

Effectively managing the risk of operations disruptions may involve making trade-offs between protecting facilities, personnel, and systems and ensuring business continuity. For example, organizations must weigh the expected costs of operations disruptions against the expected cost of implementing security protections, developing facilities, or implementing other business continuity capabilities to ensure that the organizations

---

would be able to resume operations after a disaster. Costs of disruptions can include revenues actually lost during the outage, as well as lost income because of damage to an organization's reputation resulting from its inability to resume operations. In addition, risk management guidance suggests that organizations identify potential threats that could cause disruptions, estimate the likelihood of these events, and develop their plans accordingly. By quantifying the costs and probabilities of various types of disruptions, organizations can better allocate their resources. For example, an organization whose primary site is located in a highly trafficked public area may have limited ability to increase the physical security of these facilities but could reduce the risk of disruption with a backup facility manned by staff capable of supporting its critical operations or by cross-training other staff.

---

### The Department of Homeland Security Delegated Responsibility for Protection of the Financial Sector to Treasury

The Department of Homeland Security (DHS), created to help coordinate the efforts of organizations and institutions involved in protecting the nation's critical infrastructures against terrorist attacks, has delegated to the Department of the Treasury (Treasury) this coordinating role within the banking and finance sector, which includes the insurance sector. Treasury's responsibilities include collaborating with all relevant federal, state, and local officials and the private sector. To fulfill this responsibility, Treasury coordinates with other federal officials through the Financial and Banking Information Infrastructure Committee (FBIIC), whose members include representatives of the various federal financial regulators and other related organizations.<sup>3</sup> The NAIC is a participating member of FBIIC. Treasury coordinates its collaboration with the private sector through the Financial Services Sector Coordinating Council (FSSCC), whose members include representatives from organizations such as securities exchanges, clearing organizations, and banking, securities, and insurance trade associations. For example, the American Insurance Association is a member of FSSCC.<sup>4</sup>

---

<sup>3</sup>These organizations include Treasury, the 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, Homeland Security Council, National Association of Insurance Commissioners, National Credit Union Administration, North American Securities Administrators Association, Office of the Comptroller of the Currency, Office of Federal Housing Enterprise Oversight, Office of Thrift Supervision, Securities and Exchange Commission, and Securities Investor Protection Corporation.

<sup>4</sup>The American Insurance Association is an industry association representing the interests of its members, which include approximately 450 property/casualty insurers.

---

---

## Disruptions to Insurers' Operations Could Delay Services to Policyholders, but Disruptions at State Regulators or NAIC Would Have Limited Short-Term Effects

Unless insurers maintain adequate security and business continuity capabilities, disruptions to their operations could occur that might delay the provision of key services to policyholders, such as the processing and payment of insurance claims. While a disruption at a large insurer has the potential to affect a large number of consumers and businesses, the effects would likely be limited to that insurer's policyholders and would not spread to other insurers or the larger insurance sector. Disruptions to the operations of a state insurance regulator could also delay some important services, such as licensing and product approvals for insurers and complaint resolution for consumers, but such services do not appear to be highly time sensitive, and in the short term, such disruptions would have a limited effect on insurers' normal operations. Similarly, a disruption to NAIC's operations could delay services to insurers and state regulators, but these services also do not appear to be highly time sensitive.

---

## Disruptions to Insurers' Operations Could Delay Important Services, but Limited Risk Exists of Disruption to Larger Insurance Sector

Unless insurers implement security and business continuity capabilities that adequately protect their operations from disruption and allow them to recover those operations in a reasonable amount of time should a disruption occur, important policyholder services could be delayed. Potentially disruptive events could include natural disasters, such as earthquakes or hurricanes, as well as intentional acts like bombings or computer attacks. The primary insurance services insurers provide to policyholders include assessing damage, making payments on claims or through other arrangements such as annuities, and, for health insurers, ensuring access to medical services. A disruption to any of these services has the potential to negatively impact policyholders, holding up funds needed to repair property or pay living expenses and, in some cases, cutting off access to necessary medical attention. Some large insurers have millions of policies, and while it is unlikely that all policyholders would require services at the same time, a disruption at one of these large insurers could affect a large number of people. For example, the annual report of one of the large insurers we spoke with stated that in 2004 they had approximately 65 million policies in force and handled approximately 30,000 claims a day.

The majority of insurers we spoke with generally determined the period of time customers could reasonably be without certain key services before being significantly inconvenienced and set their recovery goals for those services based on these determinations. For most property/casualty and life insurers, recovery goals for claims-processing functions were 3 days or

---

less. For most health insurers, such goals for customer service functions, including telephone information lines and authorizations necessary to receive medical services, was 1 day or less. Three of the five health insurers also told us, however, that access to critical services was not dependent on verification or preauthorization provided by the insurer, so that policyholders could obtain many critical medical services even if the insurer's operations were disrupted. For example, two health insurers said that possession of an insurance card, and not any action by the insurer, established policyholders' eligibility for medical services. This is discussed in more detail later in the report.

We also found, however, that several distinctive characteristics of the insurance industry would likely mitigate the potential effects of a disruption at one insurer, even a large company, on the rest of the insurance sector or the larger financial sector. First, limited interdependencies exist among insurers—that is, an insurer's interactions are primarily limited to those involving its own policyholders, and insurers generally do not depend on other insurers for critical business functions. Second, insurance transactions do not need to pass through a central point or process and thus are unlikely to be caught in a potential bottleneck involving the operations of many insurers. For example, in the securities trading markets, all trades must pass through an exchange and a clearing organization, creating potential single points of failure that could affect the entire securities market. In contrast, no such potential single point of failure exists in the insurance sector. Third, while there are some areas of geographic concentration of insurers, the insurance sector as a whole is geographically dispersed across the United States, making it unlikely that a single wide-scale event could disrupt the operations of a large number of insurers. For instance, a number of large insurance companies are located in New York City, but many more are located in other states. Finally, while insurers do depend on reinsurers to help them manage their level of risk, industry officials told us that the relationship is primarily financial rather than operational, and the interactions are not highly time sensitive.<sup>5</sup> Thus, a disruption at a reinsurer could delay a payment to an insurer but would not affect the insurer's normal operations. In addition, reinsurers we spoke with told us that a delay of 1 week in the payment of a reinsurance claim

---

<sup>5</sup>Reinsurance is a mechanism that insurance companies routinely use to spread risk associated with insurance policies. Simply put, it is insurance for insurance companies. Reinsurance is a normal business practice that satisfies a number of needs in the insurance marketplace, including the need to obtain protection against potential catastrophes.

---

would not have a significant negative effect on an insurer, since such claims can take anywhere from several days to years to resolve, depending on their complexity.

Of the seven insurers that told us about their experience with previous potentially disruptive events, such as the 9/11 terrorist attacks, power outages, or hurricanes, all said that the events had not caused a disruption to their operations. Those insurers that were in the areas affected by those events, even one with operations in the World Trade Center on 9/11, said that they were able to restore operations within several days and that their policyholders did not experience a disruption in their service. However, all of the insurers said that the events of 9/11 had caused them to reassess and improve their business continuity capabilities. Specifically, 13 of the insurers said that they now plan for wider-scale disruptions or have more comprehensive plans, 5 had increased their physical security, and 3 had increased the pace of previously planned business continuity improvements.

---

### Disruptions to Insurance Regulators' and NAIC's Operations Could Delay Some Services but Would Have Limited Effect in the Short Term

A disruption to the operations of a state insurance regulator could delay some services to insurers and consumers but would generally have a limited effect in the short term. Insurance regulators provide services necessary to insurers' operations—such as the licensing of agents and the approval of insurance rates and products—as well as services designed to protect consumers, such as the examination of insurers' financial solvency and conduct, and the resolution of consumer complaints. In addition, regulators may play an important role in overseeing insurers' response to policyholders' needs following a disaster. And while a disruption to a regulator's operations could delay the provision of these services, almost all of the insurers we spoke with said that a delay of even 1 or 2 weeks would likely not have a significant negative effect on insurers or consumers. For example, according to some insurers, a delay of a week or two in a regulator's approval of a new insurance product or rate would have little effect on their operations. While there are occasions when a regulator's approval is time sensitive, such as during a merger of insurance companies, such events are infrequent, and insurers do not consider them to be part of their normal operations. Similarly, state regulators' services on behalf of consumers do not appear to be highly time-sensitive. Because the resolution of consumer complaints against insurers can take several months, and examinations generally occur once every 3 to 5 years, a delay of 1 or 2 weeks would not be substantial.

---

A disruption to NAIC's operations could also delay some services to insurers and state regulators but would generally have a limited short-term effect on insurers' and regulators' normal operations. As noted earlier, NAIC provides optional automated services to both insurers and state regulators, services that were used to at least some extent by most of the insurers and regulators we spoke with. In addition, NAIC provides data collection and analysis services for state regulators, a service used by all of the state regulators we spoke with. A disruption to NAIC's operations could disrupt the provision of any of these services but would generally have only a limited short-term effect. As noted above, product and rate approvals and agent licensing did not appear to be highly time sensitive, and a delay of 1 to 2 weeks would not have a significant negative effect. In addition, several of the regulators and insurers that used these NAIC services said that if NAIC's systems were not operational, other means were available, such as e-mail and standard mail, to complete the same transactions (although less efficiently). Because the examination process is also not highly time sensitive, a delay of 1 or 2 weeks in state regulators' ability to obtain financial analyses from NAIC or use NAIC's financial database would not have significant negative effects. Finally, of the 17 insurers that commented on the potential effect of a disruption to NAIC's operations, 16 said that it would not affect their normal operations.

---

## Insurers, Most State Regulators, and NAIC Have Taken Actions Designed to Protect and Recover Their Critical Operations

Each of the insurers we spoke with, most of the state insurance regulators we met with, and NAIC all indicated that they had taken actions designed to protect their critical operations from disruption and recover them should a disruption occur. The insurers told us that they had generally implemented similar capabilities, using analyses of their own and their customers' needs to establish their business continuity plans and set their recovery time objectives. As discussed earlier, most insurers told us they could recover their most critical operations within a day and most other operations within 3 days. While each of the state regulators said they had taken steps to back up critical data, three were lacking other important elements of a sound business continuity plan, such as procedures to follow if critical computer systems were unavailable or their primary offices were inaccessible. NAIC has also taken actions to protect and recover its critical systems and told us critical operations could be recovered within 24 hours.

---

---

## Insurers Have Implemented Security and Business Continuity Capabilities Designed to Meet Their Own and Their Customers' Needs

As discussed more fully later in this report, while NAIC examination guidelines provide some criteria for insurers to use in developing their information and business continuity capabilities, they do not establish specific recovery time objectives for insurers' critical operations. To set specific recovery time objectives for their critical systems, most insurers used an analysis of their own needs or some combination of their own and their customers' needs. For example, some insurers said they had based their recovery time objectives on their need to manage their assets and liquidity, while others said they looked at the length of disruption that would be tolerable to their customers. Those using cost-benefit analyses estimated the costs of disruptions of varying lengths and compared them with the costs of different recovery time capabilities. None of the insurers we spoke with were aware of any generally accepted, industrywide recovery time objectives for insurers' operations.

Most of the insurers we spoke with said that while they generally faced the same level of threats as financial market organizations, they were less likely to be the target of intentional disruptions because they believed they had a lower public profile than many financial market organizations. That is, while insurers said they generally faced the same threats from events such as natural disasters, power outages, and computer viruses, they also said that they were less likely to be specifically targeted by terrorists, computer hackers, or others because they were not as well known publicly as certain organizations in the financial markets. In addition, most insurers also believed that the insurance sector as a whole faced a lower risk of industrywide disruptions than the financial markets, largely because—unlike the financial markets—the industry did not have a single point through which all transactions passed. A number of insurers also pointed to the geographic dispersion of insurers across the country, compared with the concentration of financial market organizations in New York City, as a reason why the overall insurance sector faced a lower risk of disruption.

The majority of insurers told us that there was less of a need for quick recovery of insurers' operations compared with other financial market organizations. For example, 10 of the 18 insurers we spoke with felt that their individual company's need to recover quickly was less than it was for other financial market organizations. In addition, most of the insurers felt that the need for quick recovery in the insurance sector as a whole was less urgent than in the financial markets. These insurers cited several reasons for this, including that most insurance transactions were less time sensitive than financial market transactions and, again, the lack of a potential single



---

point of failure in the insurance sector that could spread a disruption from one insurer throughout the industry.

### Insurers Took Similar Actions to Protect Their Operations from Disruption

Most of the 18 insurers we spoke with indicated that they had taken similar actions designed to protect their operations from disruption and meet their recovery needs should a disruption occur. First, insurers indicated that they were taking a number of similar actions designed to protect their information systems and data from theft and disruption, including hacking attempts and computer viruses. For example, all of the insurers we spoke with told us that they had implemented access controls and intrusion detection systems and did regular assessments of potential vulnerabilities in their information systems, including tests in which internal or external parties attempted to gain unauthorized access to their systems. In addition, all of the insurers indicated that they had taken steps designed to ensure their compliance with provisions of the Gramm-Leach-Bliley Act (GLBA) requiring that they protect consumer privacy information, incorporating GLBA requirements in their information security program and performing internal compliance reviews.<sup>6</sup> The insurers we spoke with reported varying levels of intrusion or hacking attempts, with one insurer stating it experienced what it considered to be “frequent” intrusion attempts, six stating they had experienced what they would consider an “average” amount of such attempts for companies such as theirs, and four reporting they had experienced only “occasional” or “infrequent” intrusion attempts. None of the insurers reported having experienced any significant disruptions or thefts as a result of intrusion attempts, viruses, or other types of potentially disruptive events.

All of the insurers had also indicated that they had implemented similar physical security protections, with most stating that the level of security at any given facility usually varied according to the perceived risks at that facility. For example, all of the insurers we spoke with utilized some combination of employee badges or scan cards, visitor stations, or security guards to protect their facilities, but at high-risk locations, such as those located in large cities, or at more critical facilities, such as computer data centers, they implemented greater physical security protections. For example, one insurer established minimum standards for most facilities that included security guards, surveillance cameras, and employee badges. In areas containing critical computer systems, however, the firm installed

---

<sup>6</sup>The information privacy provisions of GLBA are set forth in Subtitle A of Title V of GLBA, Pub. L. No. 106-102 §§ 501-510, codified at 15 U.S.C. §§ 6801-6809 (2000).

---

tailgating alarms—which are tripped if more than one person attempts to enter based on a single employee badge—and biometric devices that ensure a single employee is never alone within the area, reducing the risk that someone could cause a disruption without being observed.

**Insurers Implemented Similar Business Continuity Capabilities, Most of Which Are Designed to Recover Critical Operations within a Day**

Insurers also told us that they had implemented similar capabilities designed to restore critical operations following potential disruptions. First, all of the insurers we spoke with had separate computer backup facilities designed to be capable of running critical operations that, for almost all of the insurers, were located in different geographic areas from their primary facility. Of the 18 insurers, 14 owned their own backup facility, 3 had contracted with a vendor for backup space and computer systems at the vendor's facilities, and 1 used a combination of owned and contracted facilities. Second, at least 16 of the 18 insurers were conducting at least some critical operations at multiple geographically dispersed facilities, so that if one facility experienced a disruption, the other facilities could continue those critical operations.<sup>7</sup> Third, at least 13 of the insurers had multiple, geographically dispersed customer call centers and had the ability to immediately reroute calls to any of the call centers should one experience a disruption. Finally, at least 11 of the insurers had the capability for certain staff to log in to the company's computer systems remotely, from home or other locations, should their offices become inaccessible. Some insurers also had additional capabilities that enhanced their ability to continue operations following a disruption. For example, 4 insurers either owned or had contracted for mobile operations vehicles that could be driven to wherever they were needed. These trailers generally had full computer systems, generators, and satellite communications capabilities and could be used to conduct claims processing or other critical operations. For example, 2 of the insurers used such vehicles to set up temporary claim processing or customer service operations in areas affected by Hurricane Katrina in September 2005 to provide better access for their policyholders. Figure 1 shows an example of one such vehicle.

---

<sup>7</sup>Not all of the insurers provided complete information on their business continuity capabilities.

---

---

**Figure 1: Insurer's Mobile Operations Vehicle**

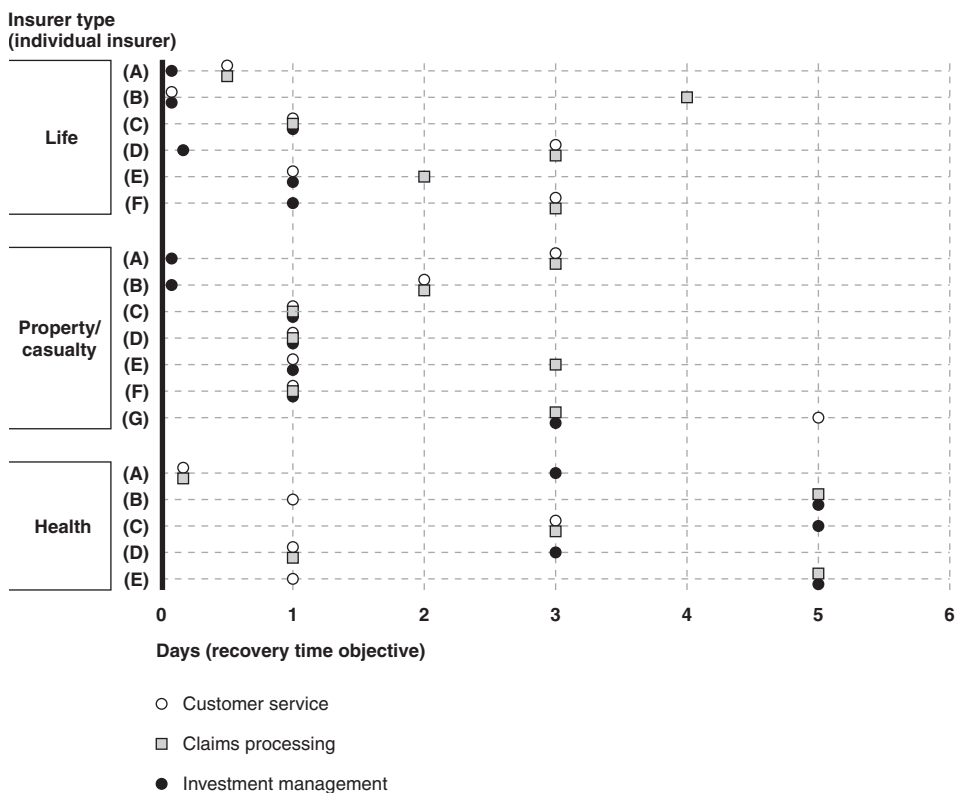


Source: Insurer (name not disclosed).

Most of the insurers told us that they were capable of recovering what they considered to be their most critical operations within 1 day, and recover most other operations within 3 days (see fig. 2). The type of operations considered to be most critical varied somewhat by the type of insurer. All of the health insurers considered customer service functions, including customer call centers and services required to receive medical care, to be one of their highest priorities, and 4 of the 5 health insurers we spoke with said they could restore such operations within 24 hours. All of the property/casualty and life insurers we spoke with considered their investment management functions one of their highest priorities, with all 6 of the life insurers and 6 of the 7 property/casualty insurers telling us they could restore such operations within 24 hours. Claims-processing operations were considered to be of highest priority by 3 of the 5 health insurers, 3 of the 7 property/casualty insurers, and none of the 6 life insurers. For a number of the insurers, the relatively low priority given to claims-processing operations was reflected in longer recovery time objectives. For example, while all 6 life insurers told us they could restore their investment management functions within 24 hours, only 2 could restore their claims-processing operations that quickly. The remaining 4 insurers needed 2 to 4 days. Similarly, while 6 of 7 property/casualty insurers said they could restore their investment management functions within 24 hours, only 3 said they could restore claims-processing operations as quickly. The remaining 4 insurers could restore such operations within 2 or 3 days. As noted earlier in this report, insurers often

set their recovery time objectives based on the length of delay tolerable to their customers; thus, while a number of insurers have longer recovery objectives for claims operations, they believe such objectives will still adequately meet their customers needs.

**Figure 2: Insurer Recovery Time Objectives for Several Insurer Functions**



Source: GAO.

Insurers indicated that they were also taking steps to help ensure the resiliency of their telecommunications capabilities and reduce the risk of a disruption to their ability to communicate and transfer data. As we have noted in a previous report, the September 2001 terrorist attacks highlighted the critical importance of resilient telecommunications services, as the resulting damage disrupted service to thousands of business and

---

residences.<sup>8</sup> We also described some of the difficulties of ensuring that telecommunications services can withstand the effects of disruptions, as well as actions taken by organizations to enhance the resiliency of their telecommunications systems, such as using diversely routed lines and circuits. All of the insurers we spoke with were also taking actions to address their need for telecommunications resiliency. Most of the insurers did so by purchasing services from multiple telecommunications carriers and obtaining contractual provisions that required carriers to ensure diverse routing of the insurer's lines. One of the insurers that did not use multiple carriers had paid to have its own private optical lines laid in a trench between its primary and backup data centers and planned on using these lines if normal telecommunications capabilities were disrupted. Three insurers also took advantage of technology that utilizes redundant fiber-optic rings whose routes are geographically and physically diverse, thus eliminating potential single points of failure.

#### Insurers Regularly Tested Their Information Security and Business Continuity Capabilities

All of the insurers we spoke with told us that they regularly tested their information security and recovery capabilities. Testing of information security systems generally involved some form of annual vulnerability assessment or penetration testing. The vulnerability assessments, which were generally done by the insurer, involved identifying potential weaknesses in the insurer's information security program that could possibly be exploited by hackers or others. Penetration testing, which was generally done by external consultants, usually involved trying to break into the insurer's information systems, just as an external hacker might do. A few insurers also gave the consultants the same level of computer access as a typical employee in order to test company protections against internal employees gaining access to systems or data for which they did not have access privileges. In addition, all insurers were making some efforts to comply with the information security requirements of GLBA, typically in the form of an annual review by an internal compliance department.

All of the insurers also indicated that they had conducted some type of annual testing of their business continuity capabilities, such as walk-throughs of their business continuity plans or tests of their backup arrangements for their data centers. Many insurers conducted scenario-based exercises that simulated particular events, such as power or telecommunications disruptions, and two insurers conducted surprise recovery tests that required certain units or facilities to activate their

---

<sup>8</sup>GAO-04-984, 17-18.

---

continuity plans with no warning. Further, some insurers had their data centers connected in such a way that they tested their recovery capabilities daily. For example, six of the insurers said that critical data was copied from its primary to its backup data center either continuously or a number of times a day, and four of the insurers were routing customer calls among several call centers in order to balance the load of calls at any one data center.

**Trend toward Increased Outsourcing by Insurers Raises Potential Concerns**

All but one of the insurers we spoke with outsourced some of their operations to at least some extent. In addition, two of the state insurance regulators said that such outsourcing was common among insurers, and two others—as well as a large industry association—noted that the trend toward outsourcing was growing. The most commonly outsourced function was software application development, with about half of the insurers outsourcing some work in this area and most of those using overseas vendors. Four of the insurers had outsourced part or all of their data centers' backup functions, and three had outsourced some portion of their claims-processing operations. In order to help ensure that information shared with vendors was safeguarded and that any backup arrangements with vendors functioned properly, all of the insurers monitored their outsourced functions to some extent. Most of the insurers required their vendors to adhere to certain information security or business continuity standards, had obtained contractual rights to audit certain aspects of vendors' operations, and had reviewed audit reports on the vendors' operations, such as Statement on Auditing Standards (SAS) 70 reports.<sup>9</sup> For example, several insurers said that they required vendors to work only on computer systems owned and maintained by the insurer or to separate the computer systems they used to do work for the insurer from other computer systems. Slightly less than half of the insurers conducted on-site visits to their vendors as part of their monitoring efforts, and a similar number said that they conducted some form of business continuity testing with critical vendors.

---

<sup>9</sup>SAS 70 reports describe audit tests performed and their results; the reports also discuss whether internal controls have been suitably designed and operate effectively.

---

---

## Most State Insurance Regulators Had Business Continuity Plans, but Some Plans Lacked Critical Elements

Three state insurance regulators had business continuity plans, but some plans lacked critical elements. Only two of five the state regulators we spoke with appeared aware of any guidance from their state regarding their business continuity capabilities. And while we did not find any laws in any of the five states requiring state agencies to have business continuity plans, the governor of one state had issued an order requiring all state agencies to have continuity of operations plans, and subsequent to our visit in another state, that state established a policy requiring all state agencies to have a business continuity plan. In addition, all of the states appeared to have an office within the state responsible for coordinating the state's response during an emergency as well as helping state agencies with their recovery plans or capabilities. In the absence of specific state requirements for the business continuity plans of state insurance regulators, we compared what the regulators had in place with guidance issued by the Federal Emergency Management Agency (FEMA) to federal executive branch agencies for use in developing contingency plans and programs for continuity of government operations.<sup>10</sup> The guidance states that continuity of operations planning is simply a good business practice and part of the fundamental mission of agencies as responsible and reliable public institutions. The guidance states that all such plans should provide procedures for conducting operations and administration at alternate operating facilities, and that such facilities should have all computer equipment, software, and other automated data processing equipment necessary to carry out essential functions.

Most of the state insurance regulators we spoke with indicated that they had business continuity plans in place to guide their actions during a potential disruption. Specifically, all of the state regulators had procedures in place to back up critical data, most had plans for how they would operate if their primary facilities were inaccessible, and most had backup computer systems. Despite these precautions, we found that some insurance regulators had not developed certain key components of a business continuity plan. For example, two did not have backup computer capabilities that could be used if their primary computer systems experienced a disruption. Officials at one state regulator said that it was the state's responsibility to provide such backup systems, and although such capabilities had been promised several years ago, they had yet to be

---

<sup>10</sup>Federal Emergency Management Agency, *Federal Preparedness Circular: Federal Executive Branch Continuity of Operations (COOP)* (Washington, D.C.; June 15, 2004).

---

put in place. In addition, two of the state regulators—including one of the regulators that had no backup computer capabilities—had no plans for what actions they would take, or how they would conduct critical operations, if their primary offices were inaccessible. Two of the state regulators we spoke with had set recovery time objectives of restoring critical operations within 2 days after a disruption, but the other regulators had set no such goals.

NAIC officials told us that they can aid state insurance regulators' business continuity efforts in two ways. First, by servicing as a repository for much of the states' critical data, including insurer financial data as well as insurer licensing and market regulatory information, NAIC acts as a backup for critical data also possessed by state regulators. Second, NAIC can provide some resources to assist state regulators in the event that a disaster or other disruption affects regulators' ability to conduct business. For example, following Hurricane Katrina in 2005 NAIC coordinated efforts to provide an automated system to capture, coordinate, and address consumer complaints.

---

## NAIC Has Taken Actions to Protect Its Operations and Recover Critical Functions Following a Potential Disruption

NAIC had taken action designed to protect its critical information systems and data, and recover its operations should a disruption occur. Because no criteria specific to NAIC exist in the areas of information and physical security, we compared NAIC's capabilities in these areas with guidance for federal agencies. To review NAIC's information security capabilities, we also compared NAIC's practices with information security guidance developed for federal agencies in the *Federal Information System Controls Audit Manual* (FISCAM)<sup>11</sup> and recommended security controls published by the National Institute of Standards and Technology.<sup>12</sup> To review NAIC's physical security capabilities, we used standards developed by the Department of Justice for federal facilities.<sup>13</sup> While business

---

<sup>11</sup>GAO, *Federal Information Systems Controls Audit Manual, Volume I: Financial Statement Audits*, GAO/AIMD-12.19.6 (Washington, D.C.: January 1999).

<sup>12</sup>National Institute of Standards and Technology, *Recommended Security Controls for Federal Information Systems*, NIST Special Publication 800-53 (Gaithersburg, Maryland; February 2005).

<sup>13</sup>See Department of Justice, *Vulnerability Assessment of Federal Facilities* (Washington, D.C.; June 28, 1995). These standards categorize facilities into five levels, with level 5 facilities having the greatest need for physical security, and are expected to implement security measures based on their risk levels.



---

continuity criteria specific to NAIC also do not exist, NAIC officials told us that they generally try to meet the same criteria as financial market organizations, such as those issued in 2003 by securities and banking regulators.<sup>14</sup> We applied this guidance, which outlines various practices related to the resumption of critical activities by key financial market organizations—including recovering those activities within the same business day, maintaining geographically dispersed resources to meet their recovery objectives, and the routine testing of recovery arrangements.

NAIC's information security efforts were reasonable since NAIC faces a low level of identified threats and its services are not particularly time sensitive. NAIC implemented numerous information security controls to help protect the confidentiality, integrity, and availability of its systems and information. For example, it required the use of passwords, user IDs, and personal identification numbers to access systems. NAIC also installed devices or software designed to detect intrusions or attempts to gain unauthorized access to their networks and systems and developed appropriate procedures for responding to information security intrusion attempts or incidents. In addition, NAIC established and maintained a security awareness and training program for its personnel and others having access to their systems and networks. Furthermore, NAIC staff periodically tested and assessed the effectiveness of its controls and overall vulnerability of its computer environment. However, it has not had an independent organization test its controls or overall computer vulnerability since 2002. Information security literature suggests that an independent organization, on an annual or biannual basis, should test security controls and the overall vulnerability of an organization's computer environment. The lack of independent testing does not give NAIC an objective evaluation of its security controls and overall computer environment vulnerability. NAIC, however, has budgeted funds for independent testing purposes in 2006. NAIC also took steps to protect its primary facility from a physical attack. For example, it monitors the exterior and interior of this facility with closed circuit televisions, requires employees and visitors to display identification while on the premises, and limits access to sensitive areas such as computer areas and telecommunication closets.

---

<sup>14</sup>Board of Governors of the Federal Reserve, Office of the Comptroller of the Currency, and Securities and Exchange Commission, *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System* (Washington, D.C.; April 2003).

---

NAIC had also implemented business continuity capabilities designed to allow it to recover critical operations within 24 hours of a disruption—even the total destruction of its primary facility. NAIC’s current capabilities include a backup computer data center—located off-site within a vendor’s facility—to which critical data is copied many times a day, allowing NAIC to restore operations at the center within several hours. The backup center has work space for six NAIC staff, is on a separate power grid from their primary facility, and is connected to the primary facility via redundant telecommunications lines. In addition, NAIC staff can connect to both the primary and backup sites from remote locations via a telephone line connection. NAIC’s business continuity capabilities also include backup power generators at its primary facility and cross-training for staff to help ensure the availability of critical skills in the event that some staff are incapacitated. Finally, the systems used by NAIC’s Securities Valuation Office can be run out of either NAIC’s primary or backup computer data centers.

NAIC told us they have tested its business continuity capabilities in several ways. First, NAIC tests its entire business continuity plan annually. Second, NAIC tests its backup power capabilities at its primary facility quarterly by shutting down the main power systems and switching over to its backup generators. Third, NAIC conducts an annual audit of both on-site and off-site backup procedures and includes a risk assessment of NAIC’s computer data center. In an actual recovery situation, NAIC was forced to restore the operations of its Securities Valuation Office when the September 11, 2001, terrorist attacks destroyed that facility. NAIC was able to restore the functions of that office quickly at its primary facility, and ran those operations from that location for 6 weeks.

---

---

## Current Laws and Regulations and State Insurance Examinations Require Insurers to Have Business Continuity and Information Security Plans but Generally Do Not Set Minimum Capabilities

Several federal laws, such as GLBA, the Sarbanes-Oxley Act of 2002,<sup>15</sup> and the Health Insurance Portability and Accountability Act of 1996 (HIPAA),<sup>16</sup> impose general information security requirements. Neither the acts nor their implementing regulations specifically prescribe steps insurers must take to ensure business continuity in the face of disruptions; they also do not require insurers to meet certain recovery time objectives with respect to the operations and systems used to maintain their business and serve customers. State insurance departments we visited examine insurers' financial solvency and market conduct to regulate the industry and protect consumers and, as part of the examination process, review the steps insurers take to protect their key information systems and data. This review fits within the examination process as part of the larger objective of reviewing insurers' internal controls over financial solvency and financial reporting systems. Similarly, while state insurance examiners also review insurers' business continuity programs, they do so as part of the larger objective of reviewing internal controls over information systems and do not require that insurers have minimum capabilities or meet minimum recovery times.

---

## Regulations and State Examinations Do Not Establish Specific Requirements for Business Continuity for Insurers

GLBA requires financial institutions, defined to include most insurance providers or companies, to protect consumers' personal financial information and limits the conditions under which such information may be distributed to third parties (such as other businesses). The Sarbanes-Oxley Act requires public companies, including insurance companies, to include a management assessment of internal controls for financial reporting. In addition, HIPAA requires the Secretary of Health and Human Services to adopt standards for the electronic exchange, privacy, and security of health information. The regulations that govern these laws outline general security and recovery guidance that insurers must address. But these laws and regulations do not outline specific information security and business continuity protections or minimum requirements to serve customers. For example, the regulations do not require insurers to take specific actions to protect or recover the financial management systems that ensure claims payment in a timely manner.

---

<sup>15</sup>Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, §§ 103, 404, 116 Stat. 745, 755-757, 789 (2002).

<sup>16</sup>Health Insurance Portability and Accountability Act of 1996, Pub. L. No 104-191, Title II, Subtitle F, §§ 261-264 (1996), 110 Stat. 1936, 2021-2034 (1996).

---

State regulators we visited examine insurers' business continuity programs, but only when reviewing internal controls over the information systems critical for insurers' financial solvency. In addition, these states do not require that insurers meet minimum recovery standards. The placement of business continuity within the context of the overall financial solvency exam poses a potential disconnect between regulators' concern over insurers' recovery capability and where business continuity fits in the state exam process. For example, regulators told us that business continuity is an important issue and that making sure insurers can recover the ability to service policyholders, particularly the processing and payment of claims, following a disruption, is of concern to regulators. However, within the financial solvency exam, state regulators review business continuity as a part of their review of information system controls, which may not result in business continuity getting the warranted attention. In contrast, examination guidelines used by federal financial regulators, published by the Federal Financial Institutions Examination Council (FFIEC), contain a separate examination handbook devoted to business continuity planning.<sup>17</sup> In addition, although state insurance regulators had informal expectations that insurers recover certain critical operations, especially claims processing, within two days of a disruption, examination guidelines do not call for examiners to review insurers' ability to meet certain recovery time objectives. As a result, a potential disparity exists between what regulators expect, and know, regarding insurers' recovery capabilities and those insurers' actual capabilities. For example, 9 of the 18 insurers had a goal of recovering their claims- processing operations within 3 or more days, which is beyond regulators' informal expectations.

On the other hand, the lack of specific recovery time objectives in the insurance sector is similar to the situation for most other financial sector organizations. For example, with the exception of the most critical organizations in the securities markets, many financial services organizations are not required to meet specific recovery time objectives for key operational and information systems. Critical organizations in securities markets—those that are unique, provide centralized functions, or have single points of failure—are required to recover within several hours,

---

<sup>17</sup>FFIEC, *Business Continuity Planning IT Examination Handbook* (Washington, D.C.; March 2003). FFIEC comprises officials from the Federal Reserve, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of Currency, and Office of Thrift Supervision.

---

but organizations such as broker-dealers are not required to meet specific recovery times. Banks are required to meet certain criteria for developing and testing business continuity plans, but not specific recovery times.

Financial solvency examinations review the accuracy and soundness of insurers' financial information and seek to protect the public by making sure insurers maintain a financial position sufficient to stay in business and meet customer needs. As part of the exam, regulators review insurers' business continuity efforts by sending insurers a series of questions from NAIC's Information Systems Questionnaire (ISQ), which insurers answer prior to the exam. The questions generally ask whether insurers' business continuity plans prioritize and cover all critical systems, provide for backup computer operations, and ensure that plan components have been tested and remain current. Examiners review the answers and then obtain documentation during the exam to verify insurers' responses. Often, state examiners will also seek other company files or records or conduct tests of their own to verify responses. Our limited review of exam workpapers found that state examiners appeared to follow NAIC's examination guidelines and collect supporting documentation to verify insurers' responses to ISQ questions.

Based on our limited review of exam workpapers and discussions with examiners and insurers, state examinations are generally limited to ensuring that business continuity plans exist, contain basic backup capabilities, and have been tested. NAIC's exam guidelines do not establish minimum business continuity or recovery capabilities; therefore, state examiners do not hold insurers to minimum recovery time frames or capabilities during their exam. Our review of a sample of state exam workpapers in this area indicated that examiners generally did not find significant weaknesses in insurer's business continuity efforts. State examinations typically occur on a 3- to 5-year cycle—a significant amount of time between examinations, during which some information may become dated. One regulator responded to the need to remain current with insurers' business continuity plans by gathering information on the plans annually. This regulator asks insurers on an annual basis to answer a business protection and continuity questionnaire that essentially uses the same questions as the ISQ. This regulator also asks insurers to provide information describing how they will provide services to customers in the event of a wide-scale disaster.

---

States Examine Insurers' Information Security Capabilities While Reviewing Internal Controls over Financial Reporting Systems

The primary objective of information security reviews by the states we visited focuses on ensuring the accuracy of financial data related to the solvency of insurance companies. That is, examiners review internal controls that are designed to ensure the accuracy of financial information and the stability of the systems that process the financial information needed, for example, for cash management and claims transactions. To understand insurers' information security protections, state examiners use ISQ questions and materials to determine the scope of the examination and then review what steps insurers take to protect management, computer application, data processing, and Internet capabilities. Examiners also make sure that insurers use computer passwords, restrict access levels to key data facilities, and protect networks and other systems from hackers and viruses. As with business continuity capabilities, examiners also seek documentation and typically conduct tests of their own to verify insurer protections. Our limited review of a sample of state exam workpapers suggested that examiners identified areas to improve insurers' information security, but examiners did not view these as significant information security weaknesses that would likely impact either consumers or the larger insurance industry.

We spoke with five state regulators and learned that three are now using outside contractors to help conduct the information systems portions of their exams. As insurers' business continuity and information security capabilities grow more sophisticated, regulators remain concerned about the ability of their examiners to review increasingly complex information systems. While three of the regulators we visited said that they had the ability to retain staff with necessary expertise, most made use of consultants that they believed possessed the technical skills and expertise needed to understand and assess insurers' systems.

Unclear Whether Examination of Outsourced Functions Is Adequate

It is unclear whether current examination practices related to state regulator's review of functions outsourced by insurers are adequate. As noted earlier, several insurers were outsourcing some or all of certain important functions—including computer systems backup and some claims-processing functions—and some insurers and regulators indicated that there appeared to be a trend toward increased outsourcing. State regulators told us that examiners seek to hold outsourced functions to the same standards as functions performed by insurers, and work in this area primarily consisted of reviewing documentation on insurers' relationships with their vendors, such as contractual audit and testing rights, and reviewing vendors' audit results obtained by the insurer. However, only one of the state regulators we spoke with had conducted any audit work at a

---

vendor facility, which for some functions might be necessary in order to hold insurers to the same standards as if they performed the functions themselves. For example, NAIC examination guidelines suggest that, as part of their review of insurers' business continuity capabilities, examiners observe manual processing procedures designed to be used in the event that computer systems are unavailable. Without visiting vendors' facilities, it is not clear that examiners can always hold insurers to the same standards as if the procedures were carried out at insurers' own facilities.

---

## Conclusions

Disruptions to insurers' operations, while unlikely to lead to wider disruptions in the insurance and overall financial sector, have the potential to inconvenience a large number of customers. However, insurers we visited generally appeared to be taking steps designed to protect their operations from disruption and prepare themselves to recover critical operations should a disruption occur. And while NAIC appeared well-prepared for a disruption, the association agreed that increasing the frequency with which they obtain external evaluations of their security controls and overall computer environment vulnerabilities could further increase their preparedness, and had already budgeted the funds to do so in 2006. In contrast, some state regulators were prepared in some areas and less so in others. All five state regulators we visited had procedures in place for backing up their data, but three regulators lacked capabilities in other critical areas. While we recognize that the effect of a disruption to a state regulator's operations would likely have a limited short-term effect, these regulators provide key services to insurers and customers. Therefore, state regulators could generally benefit from having at least basic business continuity plans to recover their operations in the event of a disruption.

While state insurance regulators indicated the importance of reviewing insurers' business continuity capabilities, current examination guidelines and practices may not fully reflect this view. Current examination guidelines place regulators' review of insurers' business continuity plans within the larger objective of reviewing insurers' internal controls, which in turn occurs as part of reviewing insurers' financial solvency. In addition, while regulators have informal expectations for how soon after a disruption insurers should be able to recover certain critical operations, such as claims processing, the examination process does not require examiners to determine whether insurers can meet these informal expectations. This creates a potential disparity between what regulators expect—and what they know—regarding insurers' recovery capabilities and insurers' actual capabilities. This may limit regulators' ability to assess

---

insurers' ability to recover critical operations within a reasonable time following a disruption.

Finally, the limited frequency with which the regulators we spoke with conducted examination work at vendors' facilities raised questions about the adequacy of current examination practices regarding functions outsourced by insurers. According to a number of insurers and regulators we spoke with, insurers are increasingly outsourcing certain business functions, including information technology operations. While insurance regulators seek to hold outsourced functions to the same standards as those performed by insurers, examining these arrangements is generally limited to reviewing documentation on insurers' outsourcing arrangements and, at least among the regulators we spoke with, rarely involves on-site work at vendor locations. Although examiners obtain audit reports and other documentation regarding vendors' internal controls, which may be sufficient in many cases, it is unclear whether in all cases examiners can review insurers' operations to the same extent without actually visiting vendors' facilities.

While the potential concerns with existing examination guidelines and practices identified above may not necessarily have resulted in lengthier disruptions to insurers' operations to date, the opportunity exists for NAIC to ensure that this remains the case. NAIC already conducts ongoing reviews of state examination guidelines and practices to ensure that they adequately address existing and emerging conditions, and frequently revises those guidelines as a result. Considering the questions and concerns raised in this report as part of that process could potentially result in improved oversight of insurers' preparedness for potential catastrophic events—whether natural or man-made—and, in so doing, help insurers to better assist consumers, businesses, and others to recover from such events.

---

## Recommendations for Executive Action

In order to ensure that state insurance regulators can continue to provide insurers and consumers with important services within a reasonable time following a potential disruption at a state insurance regulator, state regulators, working through NAIC, as well as other appropriate state officials, should take steps to ensure that state insurance regulators implement consistent, appropriate capabilities for recovering critical functions following a potential disruption.



---

In addition, in order to help ensure that NAIC continues to adequately protect its information systems, we recommend that NAIC follow through with its commitment to have an independent organization more frequently test NAIC's information security controls and the overall vulnerability of its computer environment.

Finally, although we visited a limited number of state insurance regulators, and did not observe any specific problems as a result of current examination guidelines and practices, we recommend that state regulators, working through NAIC, use their regular review of the adequacy of state examination guidelines and practices as an opportunity to consider whether any changes to the following are warranted:

- the manner and extent to which current examinations review insurers' business continuity capabilities, including the placement of business continuity within the examination guidelines and the minimum recovery time objectives for certain insurer services; and
- current examination guidelines and practices related to the review of insurers' outsourcing of critical functions.

---

## NAIC Comments and Our Evaluation

In commenting on a draft of this report, NAIC's Executive Vice President and Chief Executive Officer generally agreed with our findings and recommendations, and identified actions that NAIC had taken, or planned to take, that were consistent with those recommendations, including actions taken following Hurricane Katrina. NAIC also provided technical comments on the report that were incorporated, as appropriate.

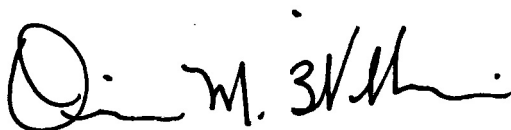
---

As agreed with your offices, unless you publicly release its contents earlier, we plan no further distribution of this report until 30 days from the report date. At that time, we will send copies to the Chair and Ranking Minority Member, Senate Committee on Banking, Housing, and Urban Affairs; the Ranking Minority Member, Committee on Financial Services, House of Representatives; the President of NAIC; and other interested congressional members and committees. We will also make copies available to others upon request. In addition, this report will be available at no charge on GAO's Web site at <http://www.gao.gov>.

---

If you or your staff have any questions about this report, please contact me at (202) 512-8678 or [williamso@gao.gov](mailto:williamso@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 III.

Sincerely yours,

A handwritten signature in black ink that reads "Orice M. Williams". The signature is written in a cursive style with a large initial "O" and a distinct "M".

Orice M. Williams  
Director, Financial Markets  
and Community Investment

---

# Objectives, Scope, and Methodology

---

The objective of this report is to describe the preparedness of key parts of the insurance industry for major business disruptions such as terrorist attacks and natural disasters. Specifically, we (1) described the potential effects of disruptions to the operations of insurers, state regulators, and National Association of Insurance Commissioners (NAIC); (2) determined what actions insurers, state regulators, and NAIC have taken to prepare for, protect against, and recover from business disruptions; and (3) assessed the extent to which certain current laws and regulations require reviews of insurers' efforts in these areas and the extent to which state examinations include such reviews. To begin addressing these objectives and obtain background information, we met with officials from insurance industry organizations representing the life, health, and property-casualty insurers.

To describe the potential effects of disruptions to the operations of insurers, state regulators, and NAIC, we interviewed officials from a judgmental sample of 18 large insurers and 5 state insurance regulators, and NAIC. We gathered information from each organization on the potential impact of disruptions on their operations, on policyholders, and on the larger insurance industry. For the purposes of our analysis, we selected large insurers by determining those with the highest total revenue in 2003 in each of the life, health, and property/casualty lines of insurance. The combined 2003 revenue of the life and health insurers in our sample represented approximately 44 percent of the 2003 revenue of all such insurers, while the combined 2003 revenue of the property/casualty insurers represented approximately 37 percent of the 2003 revenue of all such insurers. We selected state insurance regulators according to the states where those 18 insurers were located.

To determine what actions insurers, state regulators, and NAIC had taken to protect against and recover from business disruptions, we interviewed insurers, state regulators, and NAIC officials to ask what protective actions they had taken in the areas of physical security and information security. In addition, we asked about their business continuity plans, including how they were developed, of what they consisted, and how they were tested. In assessing the organizations' capabilities in these areas, we used criteria that were either established by regulators or were generally accepted by government or industry. As part of our work to assess actions taken by state regulators, we reviewed a sample of examination workpapers from each of the state regulators with whom we spoke. We attempted to review examinations of the insurers we spoke with, but were unable to do so in all cases. For our reviews, we generally relied on documentation and descriptions provided by the organizations, although we did directly

observe some security controls and business continuity elements at some insurers, some state regulators, and NAIC. We performed the most in-depth work at NAIC, where our information technology staff performed a review of information security steps NAIC had taken. Through discussions with NAIC officials and our review of NAIC's Computer and Electronic Information Security Policy and other documentation, we obtained information on NAIC's computer operating environment, including network and systems configuration, safety of key applications, and how NAIC protects points of interconnectivity between NAIC, insurers, and regulators. We also obtained information to determine whether NAIC's information security program involved risk-based policies and procedures to address security risks and how NAIC implemented logical, system access, and software change controls. In addition, we reviewed the extent to which NAIC used intrusion detection protection, periodically tested and evaluated its information security program, and had security awareness training for staff, contractors, and others with access to information systems.

To assess the extent to which current laws and regulations and state examinations review insurer business continuity efforts, we reviewed the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act of 1996, and the Sarbanes-Oxley Act of 2002, as well as their applicable regulations, to determine what each required in terms of business continuity and information security. In addition, we met with insurers, state regulators, and NAIC officials to ask how they comply with these and other regulatory requirements. When interviewing state officials, we questioned where business continuity and information fit into the examination process and reviewed state examination workpapers to determine the depth at which state examiners review insurers' business continuity efforts. During our meetings with state regulators, we reviewed a sample of examination workpapers from state financial solvency examinations of insurers and compared these materials with NAIC's examination guidelines. In most cases, state regulators provided workpapers from their most recent examination of the insurers with whom we met. One regulator, however, provided us with workpapers from examinations of other insurers with whom we had not met.

For our reviews, we relied on documentation and descriptions provided by insurers, states, and NAIC. When possible during the course of our work, we also observed controls in place for physical security, information security, and business continuity at the organizations assessed. We did not test these controls by attempting to gain unauthorized entry or access to

---

facilities or information systems, or observe testing of business continuity capabilities.

To maintain the security and confidentiality of sensitive business continuity plan information, we agreed not to name insurers or states in the report or describe their continuity or recovery efforts in ways that could identify them. Confidentiality agreements were used between us and states that requested these arrangements. We performed our work from December 2004 through October 2005 in accordance with generally accepted government auditing standards.

# Comments from the National Association of Insurance Commissioners



NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS

October 28, 2005

**EXECUTIVE  
HEADQUARTERS**

2301 MCGEE STREET  
SUITE 800  
KANSAS CITY MO  
64108-2662  
VOICE 816-842-3600  
FAX 816-783-8175

**GOVERNMENT  
RELATIONS**

HALL OF THE STATES  
444 NORTH CAPITOL ST NW  
SUITE 701  
WASHINGTON DC  
20001-1509  
VOICE 202-624-7790  
FAX 202-624-8579

**SECURITIES  
VALUATION  
OFFICE**

48 WALL STREET  
6<sup>TH</sup> FLOOR  
NEW YORK NY  
10005-2906  
VOICE 212-398-9000  
FAX 212-382-4207

**WORLD  
WIDE WEB**

[www.naic.org](http://www.naic.org)

Ms. Orice M. Williams  
Director, Financial Markets and Community Investment  
U.S. Government Accountability Office  
441 G Street, NW  
Washington, DC 20548

Dear Ms. Williams:

Thank you for the opportunity to comment on the proposed report titled "Insurance Sector Preparedness: Insurers Appear Prepared to Recover from Potential Terrorist Attacks, But Some Issues Warrant Further Review." State insurance regulators believe sound disaster response and business continuity planning is critical to the regulatory community and insurance industry's ability to respond quickly and appropriately to insurance consumers. To this end, the NAIC would like to address the recommendations outlined with the GAO's report.

First, the GAO recommends that state regulators, working through the NAIC, as well as other appropriate state officials, should take steps to ensure that state insurance regulators implement consistent, appropriate capabilities for recovering critical functions following a potential disruption. The NAIC agrees with this recommendation, as demonstrated by the work of the NAIC Catastrophe (C) Working Group and their recent update and distribution of the NAIC *State Disaster Response Plan Handbook*. The Handbook contains information on coordinating Insurance Department efforts to assist consumers with those of federal, private, industry and other state emergency assistance providers. It also has model regulations for emergency claims adjuster licensing and early access to disaster sites, sample letters for consumer and media, sample consumer service materials and guidelines for establishing procedures to expedite insurance consumer assistance for both property and life claims adjustment, and settlement mediation. The Handbook includes contributions by states such as California, Texas, Missouri, Oklahoma and Florida that have either experienced natural disasters and dealt with insurance issues that occur in the aftermath, or may have already established procedures to do so.

The Handbook does not include specific internal disaster recovery or business continuation planning, instead suggesting that internal business continuation planning should be independently undertaken by the state. However, we believe it provides key guidance for states to quickly respond to the needs of insurance

---

**Appendix II**  
**Comments from the National Association of**  
**Insurance Commissioners**

---

Ms. Orice M. Williams  
Page 2 of 3  
October 28, 2005

consumers in the event of a disaster. The states' response to hurricanes Katrina and Rita are perfect examples of how quickly and effectively the states can pool resources and expertise to organize and support disaster recovery efforts. Specifically, in response to recent hurricanes:

1. State regulators rapidly established Emergency Responder Database of state resources. This network identified consumer assistance experts from around the nation to help support state insurance department in the Gulf states.
2. A toll-free number was established to serve as a back up to assist Gulf state insurance departments with their overflow consumer calls, so that every call would be answered by a person, not an answering machine. Representatives from 14 states, along with NAIC staff volunteers, have assisted in the consumer call response effort.
3. The NAIC coordinated efforts to provide an automated system to capture, coordinate and address consumer complaints. Standardized interview forms and checklists for use in assessing consumer needs were compiled and distributed to ensure uniformity in data collection. The automated system provided regulators with the ability to spot trends and bottlenecks in the claims handling process.
4. State regulators worked with the National Flood Insurance Program (NFIP) in sorting out the portion of claims attributed to homeowners and flood insurance. The NAIC has also been an active participant in Financial and Banking Information Infrastructure Committee (FBIIC) weekly conference calls to discuss the status of disaster recovery efforts.
5. State regulators agreed to a collaborative, unified claims and loss data reporting mechanism so that insurers could direct their efforts to responding to the needs of consumers instead of responding to multiple requests for information.
6. The NAIC has been asked to by the FBI and U.S. Justice Department to participate on a Task Force to help coordinate antifraud efforts in areas affected by hurricanes Katrina and Rita. NAIC members have also met with the Coalition Against Insurance Fraud to coordinate efforts.
7. Two summits were organized to discuss regulatory response to crisis. An emergency Hurricane Katrina Summit was held on September 7, 2005 to review necessary actions of state insurance departments and insurers. Additionally, the NAIC's Catastrophe Insurance Working Group and Terrorism Insurance Implementation Working Group are scheduled to hold a National Catastrophe Insurance Summit on November 15, 2005 in San Francisco.

Nonetheless, the state regulatory community's focus on disaster recovery efforts is not complete. The NAIC will continue its work to ensure that state insurance regulators are fully prepared for potential disruptions.

The GAO also recommends that the NAIC follow through with its commitment to have an independent organization more frequently test NAIC's information security controls and the overall vulnerability of its computer environment. As you are aware, we have taken action on this recommendation, with a budget and plan for a system vulnerability assessment and security policy review by an independent consultant in 2006. The NAIC has worked very hard over the past several years, with first hand experience in responding to the collapse of the its Securities Valuation Office in New York on September 11, 2001, to ensure the

---

**Appendix II**  
**Comments from the National Association of**  
**Insurance Commissioners**

---

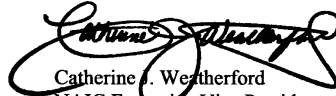
Ms. Orice M. Williams  
Page 3 of 3  
October 28, 2005

security, integrity and availability of data it collects and distributes to the regulatory community. We appreciate the GAO's findings and comments with regard to the business continuity capabilities implemented at the NAIC within the past several years. We believe the NAIC is in a very strong position to recover critical operations in a very short timeframe, most of which are critical to the state regulatory community. We agree that an independent assessment of our vulnerability to potential disruptions will provide an objective and important validation of our security and recovery plans.

Finally, the GAO recommends that state regulators, working through NAIC, use their regular review of the adequacy of state examination guidelines and practices as an opportunity to consider whether any changes are warranted in (1) the review of insurer's business continuity capabilities, including the placement of business continuity with the examination guidelines and the minimum recovery time objectives for certain insurer services and (2) the review of insurer's outsourcing of critical functions. Existing NAIC examination guidelines include provisions regarding (1) testing of the recovery plan to verify it is current and adequately tested and (2) ensuring that a restoration policy has been assigned to all significant business activities. Additionally, the guidelines include a provision regarding outside service centers, their disaster recovery plans and instructions for examiners to obtain evidence regarding audits and tests of the disaster recovery plan. The NAIC's Examination Oversight (E) Task Force of the Financial Condition (E) Committee is charged with monitoring all aspects of the financial examination process and to identify, investigate, and develop solutions to problems related to financial examinations. We believe it is important to share the GAO's recommendation to this Task Force for review and consideration.

The GAO's report and recommendations is a welcome reminder of the importance of our membership and industry's preparedness for disaster. Again, we appreciate the opportunity to comment on the draft report and provide this update on state insurance regulatory activities. Please do not hesitate to contact us if we can be of further assistance.

Sincerely,



Catherine J. Weatherford  
NAIC Executive Vice President and Chief Executive Officer



# GAO Contact and Staff Acknowledgments

---

---

## GAO Contact

Orice M. Williams, (202) 512-8678 or [williamso@gao.gov](mailto:williamso@gao.gov)

---

## Staff Acknowledgments

In addition to the contact named above, Lawrence Cluff (Assistant Director), Emily Chalmers, Kirk Daubenspeck, Patrick Dugan, Marc Molino, Stephen Ruszczyk, and Patrick Ward made key 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](http://www.gao.gov)). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to [www.gao.gov](http://www.gao.gov) and select "Subscribe to Updates."

---

## Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office  
441 G Street NW, Room LM  
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000  
TDD: (202) 512-2537  
Fax: (202) 512-6061

---

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: [www.gao.gov/fraudnet/fraudnet.htm](http://www.gao.gov/fraudnet/fraudnet.htm)

E-mail: [fraudnet@gao.gov](mailto:fraudnet@gao.gov)

Automated answering system: (800) 424-5454 or (202) 512-7470

---

## Congressional Relations

Gloria Jarmon, Managing Director, [JarmonG@gao.gov](mailto:JarmonG@gao.gov) (202) 512-4400  
U.S. Government Accountability Office, 441 G Street NW, Room 7125  
Washington, D.C. 20548

---

## Public Affairs

Paul Anderson, Managing Director, [AndersonP1@gao.gov](mailto:AndersonP1@gao.gov) (202) 512-4800  
U.S. Government Accountability Office, 441 G Street NW, Room 7149  
Washington, D.C. 20548