

United States General Accounting Office

Report to the Chairman, Subcommittee
of the Committee on Labor and Human Resources
Committee on Energy and Commerce
House of Representatives



GAO 12-111

FINANCIAL
MANAGEMENT

Greater Computer
Security Needed



124853

U.S. Department of Justice
National Institute of Justice

124853

This document has been reproduced exactly as received from the person or organization originating it. Points of view or opinions stated in this document are those of the authors and do not necessarily represent the official position or policies of the National Institute of Justice.

Permission to reproduce this ~~copyrighted~~ material has been granted by

Public Domain
U.S. General Accounting Office

to the National Criminal Justice Reference Service (NCJRS).

Further reproduction outside of the NCJRS system requires permission of the ~~copyright~~ owner.



United States
General Accounting Office
Washington, D.C. 20548

Information Management and
Technology Division

B-237674

January 5, 1990

The Honorable Edward J. Markey
Chairman, Subcommittee on Telecommunications
and Finance
Committee on Energy and Commerce
House of Representatives

Dear Mr. Chairman:

This report responds to your December 14, 1988, request and subsequent discussions with your office for information on (1) the number of known instances of hacker attempts or virus attacks on certain securities trading networks and their related systems;¹ (2) the reasonableness of existing controls used to prevent or detect the misuse of securities trading systems; and (3) the existing regulatory framework under which securities trading systems are accessed, operated, and overseen.

As agreed with your office, the systems included in this review are the Common Message Switch system and the Intermarket Trading System, operated by the Securities Industry Automation Corporation (SIAC),² and the National Association of Securities Dealers Automated Quotations (NASDAQ) system, operated by the National Association of Securities Dealers (NASD). Collectively, these systems provide vital links between the exchanges, NASD and their customers by routing orders to buy or sell stocks and options, reporting executed trades, or providing current stock pricing data to the financial marketplace.

Results in Brief

The systems described above are critical mechanisms used by the exchanges³ and NASD to disseminate information to support our nation's

¹A hacker is defined as a person who accesses or attempts to access a computer without authorization. For purposes of this report, the term hacker refers to an external threat of an unauthorized access to the networks and related systems. A virus is generally described as a computer program that can infect, replicate, and spread among computer systems. A virus can be designed to trigger a wide variety of actions, including the destruction of computer data or the disruption of computer services.

²The Securities Industry Automation Corporation is a subsidiary of the New York Stock Exchange and the American Stock Exchange, and operates automation and communications systems that, among other things, support stock trading, market-data reporting, post-trading, and surveillance activities.

³For purposes of this report, the term "exchanges" refers to the New York Stock Exchange and the American Stock Exchange.

securities trading; they must be held to the highest standards of integrity. Although no known hacker attempts or virus attacks have been reported, and sufficient controls have been established so that the risk of successful external attacks appears relatively low, we found a number of internal control weaknesses at the exchanges' and NASD's computer centers. These weaknesses pose risks of an insider threatening the systems by introducing security intrusions—such as a virus—without being detected, thus potentially threatening our nation's ability to conduct securities trading. For example, the internal controls in NASD's computer center were insufficient to protect critical software and neither computer center had internal automated data processing auditors to make sure that appropriate internal controls were in place and working.

The NASD and SIAC have generally agreed that identified weaknesses pose risks to their operations, and have already taken, or plan to take, steps to improve internal controls over these systems.

Given a continual threat of security intrusions, the Securities and Exchange Commission (SEC)—whose role, among other things, is to protect market operations from fraud—and the exchanges and NASD need to be more proactive in ensuring the integrity of these systems. In this respect, when conducting its oversight activities, the SEC does not examine the exchanges' and NASD's computer security practices. The SEC explained that it does not have sufficient technical staff to oversee the computer security practices of each of the exchanges and NASD. In addition, the exchanges and NASD do not have security administrators knowledgeable in information security and do not have comprehensive information security programs. However, the exchanges and NASD recognize the need to enhance their information security practices and are planning to establish more comprehensive security administration programs.

This report contains recommendations that SEC (1) assure that the weaknesses we found are properly corrected, (2) oversee the exchanges' and NASD's plans to expand their information security administration programs, (3) conduct or oversee assessments of the exchanges' and NASD's computer security practices, and (4) acquire the necessary technical expertise to carry out these activities.

Scope and Methodology

We conducted a risk assessment of the Common Message Switch system, the Intermarket Trading System, and the NASDAQ system. Our assessment included a review of the reasonableness of controls to protect these systems from misuse by authorized users or unauthorized intruders, and was conducted at the following organizations that own or operate these systems: the New York Stock Exchange, the American Stock Exchange, NASD, and SIAC. Our risk assessment was based on federal security standards and guidelines, and the results of consultations with selected computer security experts. Details on our assessment and our objectives, scope, and methodology are discussed in appendix I.

Background

The systems included in this review are critical to the smooth functioning of our nation's securities trading. Specifically, the Common Message Switch system provides the New York Stock Exchange and the American Stock Exchange an electronic link that receives orders for stocks and options from over 600 member firms, routes the order information to the trading floors, and, in turn, routes back trade execution information to the originating member firms. SIAC estimates that in 1988 about 80 percent of the exchanges' stock and options orders representing transactions involving more than 20 billion shares were processed over the Common Message Switch system.

The Intermarket Trading System is a nationwide communications and data processing network that links the New York Stock Exchange and American Stock Exchange, five regional stock exchanges, and the NASD for the purpose of routing stock trading orders or reports between these exchanges and NASD. By using this system, members of an exchange can participate in other markets and buy or sell stocks at the best available quotation. In 1988, trades involving 1.9 billion shares were processed over the Intermarket Trading System.

The NASDAQ system provides brokers and dealers, through about 3000 terminals, with price quotations and associated reports on securities traded through the over-the-counter market. The system's primary function is the collection, validation, and distribution of quotation information. On a daily basis, the system provides responses to inquiries, quote updates, and trade and volume reports. In addition, NASD uses the network to exchange quotations and transaction information with its counterpart exchanges in London and Singapore. In 1988, the system facilitated the trading of about 31 billion shares.

Risk of External Security Intrusions Considered to Be Low

Senior officials of SEC, the exchanges, NASD, and SIAC reported no known instances of hacker or virus attacks—attempted or successful—on the exchanges' and NASD's systems included in this review. Also, senior officials at the Department of the Treasury's United States Secret Service and the Department of Justice's Criminal Division and Federal Bureau of Investigation, had not received any incident reports and had no knowledge of any such intrusions.

The officials of the exchanges, NASD, and SIAC have implemented a wide range of security controls that protect their systems from the external threat of a hacker or virus attack and, as a result, the risk of such a threat is relatively low. These views related to the Common Message Switch system and the Intermarket Trading System were also supported by conclusions reached in a November 1988 internal review of the SIAC systems by the New York Stock Exchange.

The primary reasons for considering the risk of an external hacker or virus attack to be relatively low are that:

- The exchanges' and NASD's networks are closed networks in that access to these networks is normally through dedicated communications lines and devices that are not available to the general public.
- The systems receive data or effect transactions in a way that does not permit outsiders to input executable computer instructions necessary to execute a virus.
- The systems examine the messages received through a series of edit and sequence checks, and, if the messages are not in a prescribed format and expected sequence, they are returned to the sender for correction.
- To successfully transfer data over these networks requires knowledge and use of specialized network protocols.⁴
- Transactions involving orders to buy or sell securities that are processed by these systems are reviewed for reasonableness by automated systems, exchange professionals, or NASDAQ participants before they are acted upon. In addition, all executed securities trades receive continuous scrutiny by personnel from member firms, the exchanges, and NASD to ensure that the trades are legitimate.

In addition, these systems are not designed with features that have been successfully exploited by individuals interested in propagating a virus. For example, we reported to you in June 1989 on a virus that penetrated

⁴A protocol is a set of rules for sending data between computers or between a computer and a communications device.

the national research community's Internet system.⁵ The Internet system has a number of characteristics different from the exchanges' and NASD's systems that makes it more susceptible to a virus attack. For example: (1) it is not a closed network, rather it is a widespread, interactive, multinet network that loosely connects over 500 networks and half a million government and private sector researchers; (2) the system permitted the sending of executable computer instructions across the network, whereas the exchanges' and NASD's networks do not accept executable instructions; (3) the Internet system was exploited through weaknesses in utility programs such as electronic mail programs, and the exchanges' and NASD's systems do not process utility programs; and (4) the system offered "trusted host" features to specific users and the exchanges' and NASD's systems do not. Trusted host features allow individuals or computers to more easily access other computers.

We also found that in November 1988, the New York Stock Exchange's electronic data processing internal auditor conducted a preliminary study of the vulnerability of SIAC systems to a computer virus. For some of the reasons discussed above, the study concluded that the external risk of a computer virus being inserted either into the Common Message Switch system or the Intermarket Trading System was remote.

Computer Security Control Weaknesses Increase the Risk of an Internal Attack on Exchange and NASD Systems

The most significant threat to the exchanges' and NASD's systems—a virus, for example—is from employees who have access to their computer systems. The primary reasons for the insider threat is that these employees generally have both (1) knowledge of how the systems operate and (2) access to the systems. Overall, officials at the exchanges, NASD, and SIAC agreed with this assessment but believed that the risk of such attacks from an internal source was low because of high quality control procedures and practices in place at their computer centers. However, based on our risk assessment, we identified 10 security weaknesses at NASD and 3 security weaknesses at SIAC that increase the risk of an insider introducing a virus into the networks or related systems of the exchanges and NASD. NASD and SIAC agreed that these weaknesses posed risks to their systems, and have taken or plan to take action to correct them.

⁵Computer Security: Virus Highlights Need for Improved Internet Management (GAO/IMTEC-89-57, June 12, 1989).

NASD Security Weaknesses

To protect systems from the internal threat of security intrusions, internal controls should be in place that, among other things, (1) establish proper separation of duties involving the development, execution, testing, and review of computer programs; (2) provide stringent access controls over information and equipment used to execute computer programs; and (3) ensure accountability by documenting and retaining an audit trail of computer center activities. The need for such controls has been emphasized in federal security guidelines and consultations with selected computer security experts (see appendix I).

At NASD's computer center we found insufficient internal controls to protect against the introduction of security intrusions, such as a virus, into the NASDAQ system. Ten interrelated security weaknesses were found that included conditions where computer center staff, such as systems programmers, computer operators, or quality assurance staff (1) were able to perform tasks well in excess of their normal responsibility or (2) were performing their responsibilities in an incomplete or inadequate fashion.

Specifically, seven security weaknesses were identified in the NASDAQ system's minicomputer processing environment. These computers support several important functions including the automatic execution of small stock orders (orders of 1000 shares or fewer) and the reconciliation of stock trades. The following examples illustrate the nature of these weaknesses:

- An improper separation of duties existed between computer center functions. For example, NASD relied on systems programmers to perform certain duties normally reserved for quality assurance and applications programming staff. In addition, computer operators could perform certain duties normally reserved for security administrators. As a result, systems programmers and computer operators could more easily introduce a computer virus into production minicomputers with little chance of being detected.
- Information and equipment were not sufficiently protected to prevent computer center staff from executing unauthorized computer programs. For example, all computer operations staff had unrestricted access to production minicomputers, enabling them far greater opportunity to access data and equipment to execute a computer virus. In addition, the production minicomputers were equipped with compilers, which allowed

the opportunity for unauthorized computer programs to be more easily introduced into the system.⁶

- Documentation of the operators' activities had a short retention period. This increased the possibility of destroying audit trails, which could result in a lack of accountability or legal evidence, for example, in instances where a virus had a delayed release.

In addition to the seven minicomputer weaknesses, three other broader weaknesses were found. Within NASD's quality assurance function, software testing was either inadequate or incomplete in certain important respects. Specifically, NASD did not completely test new or modified computer programs to ensure that they did not introduce a virus. In addition, NASD did not ensure that only the tested software was entered on the production computers. We also found that NASD's physical security practices did not completely control employees' access to the computer center or their movements once inside the center. Also, NASD did not have automated data processing auditors at its computer center to ensure that proper internal controls were in place and operating as intended. Weaknesses within NASD's quality assurance, physical security, and internal auditing limit the effectiveness of its internal controls and increase the risk that its computer operations could be exploited by computer center staff.

Details of each of these internal control weaknesses have been discussed with NASD officials. They agreed that identified weaknesses pose risks to their operations and have moved swiftly to improve the controls over their system. Specifically, NASD officials responsible for NASD's computer center said that immediate actions have been taken or are planned to correct all the above weaknesses.

SIAC Security Weaknesses

At SIAC, we found three security weaknesses in the areas of software testing, contingency planning, and internal auditing. Specifically, we found that:

- The software change control staff conducted tests to ensure that new or modified software performed as intended, but did not conduct necessary tests designed to ensure that no new vulnerabilities, which would allow the insertion of a computer virus, are introduced at the time the software is developed.

⁶A compiler is an essential tool for writing an application program. It translates high-order language code into machine language that can be executed by a computer.

- SIAC had prepared a contingency plan that addressed actions to be taken if services were disrupted within the SIAC computer center. However, this plan did not include needed backup and recovery procedures in the event of a security intrusion such as a computer virus. As a result, SIAC could not ensure that exchange networks and related systems were prepared to recover efficiently from a computer virus attack. The risk of a service disruption at SIAC is of particular concern because an offsite backup facility that could be used to resume computer services in the event of a disruption is not scheduled to be operational until 1991.
- SIAC did not have any automated data processing auditors within its internal audit function. As a result, it was not well equipped to conduct necessary internal control assessments of SIAC's data security environment.

SIAC generally agreed that identified weaknesses posed increased risks to its operations and has taken or plans to take corrective actions in each area. Specifically, SIAC agreed to strengthen its software testing process. In addition, it has recently hired a computer auditor and is modifying its contingency plan to include necessary backup and recovery procedures.

SEC's Oversight and Computer Center Information Security Administration Are Incomplete

Active SEC oversight and computer center security administration activities are critical to ensuring that effective security controls are established and in place at the exchanges' and NASD's computer centers. Results of our review indicated a lack of SEC oversight in this area. In addition, we found that the exchanges' and NASD's centers had insufficient plans, policies, and procedures to define and evaluate information security controls over the exchanges' and NASD's networks and related systems.

The Securities Exchange Act of 1934 (15 U.S.C. 78a-78(jj)) provides SEC with broad authority and responsibility to oversee the operations at the exchanges and NASD. SEC may issue rules and regulations and prescribe standards and procedures to protect investors, maintain fair and orderly markets, or safeguard securities and funds. The act also provides the exchanges and NASD, as self-regulatory organizations, with broad authority and responsibility that includes (1) ensuring that the trading of securities is properly conducted, (2) issuing rules that, in general, protect investors and the public interest, and (3) assuring the prompt, accurate, and reliable performance of their functions. In this regard, the exchanges, NASD, and SIAC are responsible for controlling the access to and operations of their networks and related systems.

To help protect access to and operations of federal systems, federal agencies are required to (1) conduct risk analyses of their computer operations;⁷ (2) establish information security policies and procedures to provide reasonable network and related system protection; (3) establish a security awareness training program to make employees aware of their specific security responsibilities and how to fulfill them; and (4) conduct security certifications and audits to ensure compliance with information policies and procedures, and to ensure that security controls are in place and effectively working. Federal policy further requires that federal agencies prepare security plans for their sensitive systems.⁸ Although the exchanges and NASD are not required to follow these policies, they provide a framework to assess the reasonableness of existing controls used to prevent or detect the misuse of the exchanges' and NASD's systems. In addition, several of the computer experts interviewed recommended similar steps to ensure the effective administration of information security by the exchanges and NASD.

However, we found that SEC and the computer center managers had not established effective information security practices. Specifically, SEC oversees financial market operations through rule reviews, inspections, and surveillance activities. Among other things, SEC oversight is intended to protect against trade manipulations or fraud. It does not specifically examine the exchanges' and NASD's computer centers or their networks during these oversight activities to ensure that these centers and networks are protected from security intrusions. In discussing the need for such assessments, SEC explained that it does not have sufficient technical expertise to conduct such reviews and relies on the exchanges and NASD to ensure information security over their own systems.

Our review of the exchanges' and NASD's computer centers indicated that security administrators were primarily responsible for ensuring reasonable physical security practices, and they were not knowledgeable in information security. NASD and SIAC acknowledged that they had not established a formal information security program. For example, they

⁷According to Office of Management and Budget Circular A-130 Management of Federal Information Resources, dated December 12, 1985, the objective of a risk analysis is to provide a measure of the relative vulnerabilities of and threats to an installation, such as a computer center and its related networks and systems, so that security resources can be cost effectively deployed to minimize potential loss. Risk analyses should be conducted prior to approval of a system's design specifications, whenever a significant installation change occurs, and at periodic intervals established by the organization.

⁸Office of Management and Budget Bulletin Number 88-16, Guidance for Preparation and Submission of Security Plans for Federal Computer Systems Containing Sensitive Information, dated July 6, 1988.

had not: (1) conducted formal risk analyses of the information security threats to and vulnerabilities of their networks and systems; (2) prepared written information security plans, policies, and procedures; (3) conducted information security awareness training; or (4) conducted network and related system security certifications and audits.¹¹

NASD and SIAC had not established more formalized information security programs because they believed that the integrity of information processed by their systems was protected through a number of controls including strict data formats and protocols, and close scrutiny of the trading, reporting, and clearing of systems' transactions. Nevertheless, NASD and SIAC officials agreed with the need to establish more formal information security programs, and have begun actions to establish comprehensive information security programs for their computer center operations. NASD and SIAC have or plan to appoint information security administrators, conduct risk analyses, establish formal information security policies and procedures, conduct information security awareness training, and conduct related system security audits.

Conclusions and Recommendations

The risk of outside intrusions to these systems that support our nation's financial marketplaces is relatively low. The risk of a security intrusion by an insider is higher than necessary in these systems that are so vital to our financial well-being. SEC's limited oversight of these systems coupled with the lack of comprehensive security administration at the computer centers of the exchanges and NASD have contributed to the vulnerabilities we found. The threat of computer viruses has magnified the need for high standards of integrity for these systems. Such a security intrusion introduced into these systems could literally bring securities trading to a halt.

Accordingly, we recommend that the Chairman of the Securities and Exchange Commission:

- Immediately follow up on the security weaknesses identified in this report to ensure that they have been corrected.
- Oversee the exchanges' and NASD's plans as they expand the role of their computer security administration functions. Specifically, SEC should require that they: (1) conduct periodic risk analyses; (2) develop written

¹¹During calendar year 1989, both the New York Stock Exchange and the NASD contracted with external audit organizations to conduct system reviews that included security assessments of the exchanges' and NASDAQ systems. These results were not available at the time of our review.

-
- information security plans, policies and procedures; (3) conduct information security awareness training; and (4) obtain independent assessments of the reasonableness of network security controls.
- Periodically conduct or oversee independent assessments of the exchanges' and NASD's information security programs to ensure that they provide reasonable assurance that the networks and systems are adequately secured.
 - Acquire the necessary technical expertise to conduct these activities.

We discussed the contents of this report with senior officials of the SEC, the New York Stock Exchange, the American Stock Exchange, NASD, and SIAC, who generally agreed with our findings and recommendations. We have incorporated their comments as appropriate. In this regard, on November 16, 1989, the SEC published an automation review policy statement that, among other things, requests that the exchanges and NASD periodically assess the vulnerability of their automated systems to external and internal threats. This policy statement was not available for our review at the time we concluded our study.

As arranged with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until January 31, 1990.

This work was performed under the direction of Howard G. Rhile, Director, General Government Information Systems, who can be reached at (202) 275-3455. Other major contributors are listed in appendix II.

Sincerely yours,



Ralph V. Carlone
Assistant Comptroller General

Contents

Letter	1
Appendix I Objectives, Scope, and Methodology	14
Appendix II Major Contributors to This Report	17

Abbreviations

GAO	General Accounting Office
IMTEC	Information Management and Technology Division
NASD	National Association of Securities Dealers
NASDAQ	National Association of Securities Dealers Automated Quotations System
SEC	Securities and Exchange Commission
SIAC	Securities Industry Automation Corporation

Objectives, Scope, and Methodology

Our objectives were to obtain information on (1) the number of known instances of hacker attempts or virus attacks on selected exchange and NASD networks and their related systems; (2) the reasonableness of existing controls used to prevent or detect the misuse of exchange and NASD systems; and (3) the existing regulatory framework through which exchange and NASD systems are accessed, operated, and overseen. The systems included in this review are the Common Message Switch system and the Intermarket Trading System, operated by SIAC, and the NASDAQ system, operated by NASD.

To determine the number of known instances of hacker attempts or virus attacks on the Common Message Switch system, Intermarket Trading System, and NASDAQ system, we obtained information from senior officials at the New York Stock Exchange, American Stock Exchange, NASD, and SIAC on the extent of such security intrusions on the exchanges' and NASD's systems. We also obtained supporting information from the SEC and senior officials at the Department of Justice's Criminal Division and the Federal Bureau of Investigation, and the Department of the Treasury's United States Secret Service.

To assess the reasonableness of existing controls for preventing or detecting system misuse by authorized users or unauthorized intruders, we conducted a risk assessment to evaluate the controls used by the exchanges, NASD, and SIAC to protect their systems. At present, regulations of the exchanges, NASD and SEC do not provide specific computer security standards for securities trading systems, nor do they describe what constitutes an effective information security program. While the exchanges, NASD, and SIAC are not required to implement federal standards, these standards do provide a framework to assess the reasonableness of existing controls used to prevent or detect the misuse of the exchanges' and NASD's systems. Accordingly, we developed our risk assessment guide from a review of existing federal standards and guidelines on network and computer security. In addition, we held discussions with selected computer security experts on the need for selected security controls on the exchanges and NASD systems. Specifically, the experts we consulted were:

Federal Government

Lieutenant Colonel George Mundy, Chief Scientist, Defense Data Network, Defense Communications Agency

Ms. Judith A. Parks, Assistant Commissioner, Information Resources Systems, General Services Administration

Mr. John Perry, Special Agent-in-Charge, Fraud Division, United States Secret Service

Dr. William Scherlis, Program Manager for Software Technology, Defense Advanced Research Projects Agency

Mr. Dennis D. Steinauer, Manager of the Computer Security Management and Evaluation Group, Computer Security Division, National Institute of Standards and Technology

Private Sector

Mr. Robert P. Campbell, President, Advanced Information Management, Inc.

Mr. Albert Decker, Partner-in-Charge, Information Technology Security Services, Coopers & Lybrand

Mr. C. Howie Hodges, II, Division Manager, Risk Management Center/ Security and Risk Management Division, American Bankers Association

Dr. Clifford Stoll, Astrophysicist, Harvard-Smithsonian Center for Astrophysics.

In addition, we evaluated a confidential study conducted by the New York Stock Exchange entitled "Understanding the Threat of Computer Viruses in the New York Stock Exchange Computer Systems," (Nov. 1988).

The primary federal standards and guidelines that we used to assess the reasonableness of the controls established by the exchanges, SIAC, and NASD are the Office of Management and Budget Circular A-130, Management of Federal Information Resources, (Dec. 12, 1985), and related Federal Information Processing Standards Publications published by the Department of Commerce's National Institute of Standards and Technology. We also used guidelines contained in the Electronic Data Processing (EDP) Examination Handbook, issued by the Federal Financial Institutions Examination Council.¹

¹The Federal Financial Institutions Examination Council was established in 1978 to develop uniform examination and supervision practices for all depository institutions' regulatory agencies. Members of the Council include the Federal Reserve System, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, Federal Home Loan Bank Board, and the National Credit Union Administration.

In designing our risk assessment guide, we considered two types of threats involving hacker attempts or virus attacks. The first of these threats is the external threat that comes from unauthorized persons outside the organization.² The second type of threat is the internal threat that comes from employees inside an organization. An organization's information security program should also address emergencies such as fires, floods, electrical disruptions, etc., to the extent that such emergencies increase the external or internal threat. For each of the internal and external threats, we assessed the extent to which security controls were in place to protect the networks and related systems from hacker attempts or computer virus attacks by unauthorized persons or by authorized employees of the exchanges and NASD.

To examine the reasonableness of the exchanges' and NASD's security against these threats, we conducted our risk assessment at their computer centers and evaluated the following seven management information functions: communications management, computer programming, computer operations, quality assurance, physical security, security administration, and internal reviews.

To obtain information on the existing regulatory framework and to identify policies and procedures specific to exchange network security, we obtained appropriate regulations and interviewed officials from SEC, the New York Stock Exchange, the American Stock Exchange, NASD, and SIAC. In this regard, we reviewed available implementing procedures detailing oversight, operations, and access responsibilities.

We conducted our review in accordance with generally accepted government auditing standards between February and October 1989.

²Our assessment of the external threat to the exchanges' and NASD's networks did not include the exchanges' and NASD's member brokerage firms which, as authorized users, are responsible for the use and protection of their computer terminals and lines connected to the networks.

Major Contributors to This Report

Information
Management and
Technology Division,
Washington, D.C.

Richard J. Hillman, Assistant Director
William D. Hadesty, Technical Specialist
Robert C. Sorgen, Evaluator-in-Charge
Tamara J. Ealey, Computer Scientist

Office of the General
Counsel, Washington,
D.C.

Raymond J. Wyrsh, Senior Attorney

UNITED STATES
GENERAL ACCOUNTING OFFICE
WASHINGTON, D. C. 20548

0
Permit No. G100

First-Class Mail
Postage & Fees Paid
GAO
Permit No. G100