

GAO

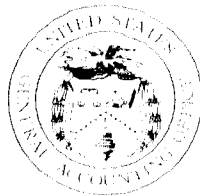
United States General Accounting Office

Report to the Chairman, Subcommittee
on Telecommunications and Finance,
Committee on Energy and Commerce,
House of Representatives

January 1990

ELECTRONIC FUNDS TRANSFER

Oversight of Critical Banking Systems Should Be Strengthened



RESTRICTED—Not to be released outside the
General Accounting Office unless specifically
approved by the Office of Congressional
Relations.

547398/

RELEASED

Information Management and
Technology Division

B-233685

January 4, 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 is in further response to your December 14, 1988, request for information concerning the adequacy of our nation's regulatory structure to oversee the security afforded to the FEDWIRE system, operated by the Federal Reserve System, the Clearing House Interbank Payments System (CHIPS), operated by the New York Clearing House Association, and the S.W.I.F.T. telecommunications system, operated by the Society for Worldwide Interbank Financial Telecommunication S.C. On February 1, 1989, we provided you with (1) descriptions of each banking system, (2) information on the federal regulatory agencies providing oversight over these systems, and (3) documentation on generic risks in using electronic funds transfer systems.¹ This report includes our assessment of the security measures in place to protect these systems from misuse and provides updated information from the regulatory agencies on their authority to oversee each system.

Results in Brief

National and international wholesale electronic funds transfers² are carried out by two systems—FEDWIRE and CHIPS, which transfer over 1 trillion dollars daily. A third system, S.W.I.F.T., is a major international message processing system that is used by banking institutions to initiate electronic funds transfers. These systems connect thousands of financial institutions located worldwide and support a number of financial activities including cash management, securities trading, corporate funds transfers, foreign exchange, U.S. dollar clearing, and international banking transactions.

There have not been any reported incidents of fraudulent electronic funds transfers over these systems by the employees who operate or

¹Electronic Funds Transfer: Information on Three Critical Banking Systems (GAO/IMTEC-89-25BR Feb. 1, 1989).

²Wholesale electronic funds transfer generally refers to a funds transfer used to satisfy an immediate, high-dollar obligation, or to enable the recipient to make immediate use of the funds.

oversee them. However, the results of our review of the security measures in place to protect these systems from misuse have not been satisfying. Given that these systems have become the foundation for international and domestic funds movements, they should have stringent security provisions and effective regulatory oversight. We did not, however, always find these levels of security and oversight. Although these systems, to varying degrees, have safeguards in place to facilitate the timely and secure processing of financial transactions, we found instances of computer control weaknesses and other management weaknesses that, if exploited, increase the risks to these systems of a disruption or degradation of services or the unauthorized use, modification, destruction, or disclosure of data.

With FEDWIRE, for example, we found weaknesses in the management of software that controls access to the system, and additional weaknesses involving physical security, computer operations, and other areas. With CHIPS, the weaknesses included inadequacies within security administration and quality assurance that increased the risk of unauthorized use, modification, or destruction of data. With S.W.I.F.T., we found a potential computer capacity problem with the existing system, and system development problems with a planned replacement system. With both CHIPS and S.W.I.F.T., we found weaknesses that adversely impact on the independence of the internal audit functions.

Officials who manage these systems have generally agreed that the weaknesses we identified pose increased risks to their operations and have taken or plan to take steps to improve controls over these systems. In particular, officials managing FEDWIRE and CHIPS have moved quickly to correct identified weaknesses, which demonstrates a strong commitment to providing for secure and reliable operations. We believe the S.W.I.F.T. organization is equally committed to providing secure and reliable services, but their weaknesses are generally more complicated and require continued management attention to satisfactorily resolve.

We also found that the oversight over these systems was uneven. For example, the Federal Reserve Board does not require periodic external security reviews of FEDWIRE even though the last such review conducted in 1983 disclosed a number of security weaknesses. The regulatory agencies believe, and we concur, that they have the authority to oversee CHIPS, and these agencies regularly review CHIPS operations on a joint basis. CHIPS, however, does not recognize this authority. Its position is that these reviews are done on an invitational basis. No examinations

have been carried out on the S.W.I.F.T. system, and the regulatory agencies are uncertain as to whether they have this authority.

This report includes recommendations to federal regulators to strengthen the oversight of FEDWIRE and CHIPS and to work with the international banking community to assign responsibility for ensuring effective oversight and regulation of the S.W.I.F.T. system.

Scope and Methodology

We conducted a risk assessment of the security of the FEDWIRE and CHIPS systems that included 16 critical organizational functions considered to be essential to the secure processing of electronic funds transfers. Our assessment was based on provisions within federal standards and guidelines and audit guidelines of the Federal Reserve Board and related banking groups. We were unable to conduct a complete assessment of the S.W.I.F.T. system because the organization that operates it, a Belgian cooperative society, limited our access to information and supporting system documentation. As agreed with your office, we did not review the level of security provided by depository institutions—such as commercial banks—over the operation of their terminals connected to these systems. We also obtained written opinions from and interviewed officials of the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Federal Reserve Board on their authority to examine the CHIPS and S.W.I.F.T. systems. Details of our scope limitation on the S.W.I.F.T. system and our objectives, scope, and methodology are included in appendix I.

Background

FEDWIRE has been in existence in some form since 1918, and is the nation's primary wholesale electronic funds transfer system used by the banking community to handle the payments banks make to each other on behalf of themselves and their customers within the United States. It is also used to transfer U.S. government and federal agency securities in book-entry form.³ In 1988, FEDWIRE served over 11,000 depository institutions and government agencies and processed 66 million transfers valued at \$253 trillion.

CHIPS has been in existence since 1970 and is the primary wholesale electronic funds transfer system that supports the international transfer of

³A book-entry security generally is not available in physical form. Rather, it exists as an entry on the books of the obligor or its agency. FEDWIRE is used to transfer these securities between depository institutions.

funds between United States and international banks. This private sector system electronically links depository institutions and branch offices of foreign banks, all of which are located in New York City, and serves as a conduit for moving dollar transactions including letters of credit, collections, reimbursements, foreign exchange transactions, and the sale of short-term Eurodollar funds. In 1988, CHIPS served 139 national and international depository institutions and processed about 34 million transfers valued at \$165 trillion.

The S.W.I.F.T. telecommunications system, operational since 1977, is owned and operated by a Belgian cooperative society. It is a major international message processing system used by banking institutions worldwide to transmit information that is critical to initiating international electronic funds transfers through CHIPS and FEDWIRE.⁴ As of December 1988, the system provided more than 70 types of messages including international payments, statements, and other transactions associated with international finance. Also, the S.W.I.F.T. organization has recently developed new message types to allow for the international trading of securities. During 1988, 24 brokers, exchanges, and settlement institutions from the securities markets in New York, Tokyo, and London were approved as S.W.I.F.T. participants. In 1988, S.W.I.F.T. served 2,537 financial participants and processed 255 million messages. Statistics on the messages' value are not maintained.

Computer Control and Other Management Weaknesses Identified at FEDWIRE, CHIPS, and S.W.I.F.T.

There have not been any reported incidents of fraudulent electronic funds transfers over the FEDWIRE, CHIPS, and S.W.I.F.T. systems by the employees who operate or oversee them. However, during our review we have identified a number of weaknesses that could adversely affect their operations. Officials who manage these systems have generally agreed that identified weaknesses pose increased risks and have taken or plan to take steps to improve the controls over these systems.

FEDWIRE Control Weaknesses

Our risk assessments of FEDWIRE identified a total of 17 control weaknesses at the four Federal Reserve banks we visited, and two systemwide weaknesses that, if exploited, could adversely affect the smooth functioning of portions of the FEDWIRE system. Table 1 shows the 10 functional areas where certain specific weaknesses were identified.

⁴The S.W.I.F.T. system is one of a limited number of systems that is growing in importance within the international banking community and the global securities marketplace for providing critical electronic message processing services.

Table 1: Control Weaknesses Identified at Federal Reserve Banks

Functional Area	Federal Reserve Banks			
	New York	San Francisco	Chicago	Dallas
Security Software Management	x	x	x	x
Physical Security	x	x		x
Computer Operations		x		x
System Software Management	x	x		
Capacity Planning			x	
Contingency Planning		x		
Quality Assurance				x
Communications Management		x		
Network Management			x	
Wire Room Operations	x			

Specific weaknesses we identified at two or more reserve banks are briefly discussed below:

- At all four banks the software that allows access to FEDWIRE was not properly controlled by the security administration function in accordance with Federal Reserve System policies in that the receipt, testing, modification, and installation of the security software was being performed by systems programmers. This reduces the level of control over this software and increases the risks of unauthorized access and changes to sensitive software or data.
- At three banks there were inadequate physical security provisions including surveillance devices such as cameras or motion sensors to monitor the activities within critical processing areas. At one of these banks the electronic card key device that records when employees exit from the computer center was inoperable. This weakens the banks' ability to monitor activities of computer center staff.
- At two banks there were computer operations weaknesses, including the lack of a back-up power supply at one bank, to support operations during short-term and long-term power outages. Also, the ability to access critical computer commands at another bank was not limited to operations personnel. This increases the risk of a disruption in services and unauthorized disclosure of information.
- At two banks system software which, among other things, operates and controls the FEDWIRE system, was not being properly reviewed by the data security administration group or certain employees had excessive access privileges. Both of these circumstances increase the banks' susceptibility to unauthorized use or modification of FEDWIRE resources.

Additional weaknesses found at only one reserve bank included (1) operation of the central processor of FEDWIRE at excessive utilization levels, (2) an incomplete disaster recovery manual and the discontinuance of disaster recovery planning and testing, and (3) the need to enhance the protection of code words used to verify funds transfer instructions within a funds transfer wire room. Operation of FEDWIRE hardware at excessive utilization levels could cause degraded service including transaction processing delays and software problems. By not maintaining currency in its contingency planning, testing, and documentation, one bank increases the potential for prolonged service disruptions from earthquakes, power outages, etc., that could disable its primary processing center. Insufficient procedures for safeguarding funds transfer code words increase another bank's risk of the unauthorized disclosure of data or the initiation of a fraudulent funds transfer.

Officials who manage FEDWIRE generally agreed that the above control weaknesses pose increased risks to their operations, and have taken or plan to take corrective action. Details of these weaknesses and the status of corrective actions are discussed in appendix II.

The two systemwide weaknesses that limit the effectiveness of the controls environment over FEDWIRE involve (1) the lack of a requirement to conduct periodic external system security reviews and (2) incomplete use of recommended telecommunications security controls to protect against the unauthorized disclosure and modification of FEDWIRE transactions. The lack of periodic external security reviews could enhance the likelihood of not detecting control weaknesses. The last external review, conducted by a consulting firm in 1983, proposed a large number of safeguards to improve FEDWIRE security and overall operations. For example, this review identified the need for the following additional telecommunications security controls: (1) encryption to protect FEDWIRE transactions against unauthorized disclosure, and (2) message authentication to ensure that transactions have not been altered during transmission.

Officials who manage FEDWIRE also generally agreed that these systemwide weaknesses pose some risk to their system. Although the Federal Reserve Board places a high degree of confidence in its own reviews, it agreed to consider conducting periodic external security reviews. With regard to the telecommunications security controls suggested in the 1983 external review, encryption is being used to prevent disclosure of information during transmission between Federal Reserve banks and the depository institutions they serve, and the Board is

studying proposals to encrypt transmissions between Federal Reserve banks. Message authentication is also being used between the Department of the Treasury and the Federal Reserve Bank of New York, and the Federal Reserve is prototyping the use of message authentication devices at four of its banks. It expects to complete the prototyping exercises in December 1989.

Concerns With CHIPS' Controls

The CHIPS controls environment was relatively strong; however, our risk assessment of the CHIPS system identified three weaknesses that require corrective actions. As discussed below, these weaknesses involved the performance of incompatible duties within CHIPS' quality control group, a lack of an independent internal audit function, and a lack of complete external audit coverage.

- The CHIPS quality control group performs incompatible duties related to (1) testing, approving, and installing new computer programs; (2) administering system passwords; and (3) reviewing and investigating security violation reports. Combining duties such as these within one organizational function is contrary to generally accepted practices. To reduce the risk of unauthorized modification or destruction of data, different organizational units should be responsible for testing software and administering security.
- The placement of the internal auditor within the CHIPS' organizational structure could adversely affect the auditor's independence. CHIPS' policies require an independent audit function. Although the CHIPS internal auditor officially reports to an office outside of the data processing department (1) on a day-to-day basis the auditor reports to the Senior Vice President of Data Processing, (2) the Senior Vice President of Data Processing participates in preparing the internal auditor's annual performance appraisal, and (3) the auditor's salary is paid from the data processing department's budget. Such practices can weaken the independence and objectivity of the internal audit function.
- Although limited scope external reviews have been conducted about once every 2 years, CHIPS data processing operations have not been subject to a complete external review that includes an opinion on the reasonableness of CHIPS controls. As a result, system weaknesses could go undetected or not be corrected in a timely manner.

Senior CHIPS officials agreed that these weaknesses increased risk to their system. In this regard, they have recently established a security administration function to, among other things, administer system passwords and review security violation reports. In addition, they have

implemented a set of controls to properly control testing, approving, and installing computer software. Officials also plan to take action to comply with the CHIPS policy requiring an independent audit function and intend, for example, to separate the internal auditor's salary from the data processing department's budget. These officials also plan to contract for a comprehensive external review.

S.W.I.F.T. Internal Control Weaknesses and Other Concerns

We were unable to conduct a complete assessment of the level of security afforded to the S.W.I.F.T. system. However, our limited risk assessment disclosed three areas of concern involving (1) the independence of the organization's internal audit function, (2) potential computer capacity problems with the existing system, and (3) system development problems with a planned replacement system. Specifically:

- Although the S.W.I.F.T. system is subjected to regular external security reviews, its internal audit function is not independent. Specifically, this function is responsible for both (1) the performance of audits of the system on a periodic basis to ensure that messages transmitted are secure, accurate, and timely; and (2) the design and installation of security features on the S.W.I.F.T. system. Since the same individuals have both audit and security responsibilities within the same organization, independent assessments of security policies and practices cannot be performed.
- The S.W.I.F.T. organization has taken a series of steps to increase the capability of the existing system to process increasing transaction volumes. However, because of continued growth in work load, the system is expected to reach its capacity in 1991. In addition, given design limitations, the capability of the system to continue to accommodate expected traffic increases has been questioned by the organization's external auditors. System performance problems associated with overloading systems like S.W.I.F.T. include degradation of service levels that could significantly increase the time required to process transactions in portions of the system. As a result, the S.W.I.F.T. system could encounter sporadic instances where transactions are delayed or it may be unable to accommodate new business. Such events could necessitate adjustments in cash management practices of international banks and constrain services provided by the international banking community.
- The S.W.I.F.T. organization is in the process of developing an enhanced system referred to as S.W.I.F.T. II. This replacement project is currently 2-3 years behind schedule because of several factors including (1) software development problems, (2) organizational and management problems, and (3) security concerns. Concerns raised in the most recent

external audit report on the replacement system included system performance problems including system availability and functionality shortfalls, and a lack of formalized system testing procedures. S.W.I.F.T. officials believe that significant strides have been made to correct system development problems, but to ensure safe and reliable message processing, December 1989 plans to begin operating the new system were delayed. With continued system development problems, capacity concerns associated with overloading the existing system are heightened.

S.W.I.F.T. officials agreed that its internal audit function was not independent, but believed that the regular external security reviews mitigated this weakness. These officials also acknowledged that, as the S.W.I.F.T. system expands in the future, the organization may have to establish an independent audit function. These officials also agreed with us that the current system will reach its capacity limits in 1991, but believed that the new system will be operational before then.

Legal Framework and Oversight of Electronic Funds Transfer Systems

The Federal Reserve System has the dual responsibility of providing electronic funds transfer services through FEDWIRE and regulating and examining funds transfers and other activities of Federal Reserve banks, branch offices, and member depository financial institutions. Oversight of FEDWIRE is conducted by the Federal Reserve Board primarily through annual financial examinations and operations reviews of a bank's activities at least once every 3 years. Overall results of the examinations and reviews of the FEDWIRE system have generally disclosed that it has a good performance record, and that comprehensive standards, policies, and procedures governing critical processing activities have been adopted.

The Federal Reserve Board, Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency have specific regulatory and oversight responsibilities over U.S. banks. These banking agencies point to section 7(c) of the Bank Service Corporation Act, as amended, 12 U.S.C. section 1867(c), as the primary basis for them to regulate and examine the performance of certain traditional banking services (e.g., clerical, bookkeeping, accounting, statistical, or similar services) that are provided to a regulated bank by another entity or organization.

Two of the banking agencies also referred to section 8(b) of the Federal Deposit Insurance Act, as amended, 12 U.S.C. section 1818(b), as another basis on which they could correct problems regarding services

provided to regulated banks. Under this section, the banking agencies may prohibit a regulated bank from engaging in any unsafe or unsound practices and procedures. This could be accomplished either through “cease-and-desist” proceedings against a bank or through regulation.

On the basis of these acts, the banking agencies generally believe, and we concur, that proper authority exists for the regulation and examination of CHIPS operations and activities. For example, the Federal Reserve Board states that the primary services offered through the system are traditional banking functions, as set forth in the Bank Service Corporation Act. In addition, the Board believes that funds transfers over the system have a substantial effect on bank balance sheets and have the potential to pose significant risk to a bank using the system should problems develop. The Office of the Comptroller of the Currency also believes that CHIPS activities may reasonably be classified as “clerical, bookkeeping, accounting, statistical, or similar functions” within the meaning of the Bank Service Corporation Act.

Because the clearing function provided by the New York Clearing House Association—the operators of CHIPS—is not specifically identified in these acts, officials of the Association do not agree that the acts authorize any federal banking agency to regulate or examine CHIPS. Nevertheless, the Association allows examinations of the system to be conducted on an invitation basis. Examinations are conducted jointly about every 18 months by a team of examiners from the Federal Reserve Bank of New York, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency. Since the Association has cooperated with the banking agencies, there has been no need to resolve this question to date. In their examinations, the regulators have reported that CHIPS generally adheres to high computer security standards.

We agree with the consensus of the banking agencies regarding their regulatory and examination authority over CHIPS operations and activities, essentially for the same reasons the agencies have stated. The services that CHIPS provides regulated banks appear to us to fall within the types of banking services covered in the Bank Service Corporation Act (e.g., clerical, bookkeeping, accounting, statistical, or similar services).

The banking agencies have never regulated or examined the S.W.I.F.T. system. However, the agencies generally agree that while it is somewhat less clear, a reasonable case can be made that the Bank Service Corporation Act authorizes them to review S.W.I.F.T. operations. Specifically, the

Office of the Comptroller of the Currency believes that the act authorizes the regulation and examination of the system's operations and activities. The Federal Deposit Insurance Corporation and the Federal Reserve Board are somewhat less affirmative. The Federal Deposit Insurance Corporation, for example, states that the services provided by the system seem a step removed from the concept of core banking functions, but are closely related to traditional banking functions and have potential significance for bank safety and soundness. The Corporation therefore believes that it is plausible to argue that S.W.I.F.T. services fall within the purview of the act.

The Board states that the S.W.I.F.T. system provides primarily a communications service and that while its messages form the basis for payment transactions, the system does not directly transfer funds between banks, and therefore, does not present the same risks as CHIPS transfers. The Board also pointed out that the S.W.I.F.T. system can be viewed as a telecommunications system dedicated to communicating financial information, and that telecommunications services provided to banks historically have not been examined by the banking agencies. In addition, the Board believes that any review of the system would be complicated since its headquarters is in Belgium, and the majority of its members are foreign banks whose foreign offices are not subject to examination by U.S. bank regulatory agencies. Nevertheless, the Board did recognize that S.W.I.F.T.'s close relationship to payment activities may necessitate the need for examinations at some point in the future.

In discussing these matters with a senior S.W.I.F.T. official, we were told that, notwithstanding the above uncertainties, S.W.I.F.T. management would cooperate with regulatory authorities to resolve any concerns they may have over the security and reliability of its systems. As an example of the S.W.I.F.T. organization's participation in the past in resolving issues involving international coordination, the official stated that the S.W.I.F.T. organization has met with the Bank for International Settlements to discuss developments in international banking and to exchange information to resolve important and sensitive banking issues.⁵

⁵The Bank for International Settlements is a prominent international organization, located in Switzerland, that has served as a major forum for central bank governors to meet to address jointly many international financial and economic issues. The United States and 11 other nations participate in regular meetings at the Bank for International Settlements. The United States' representatives include officials from the Federal Reserve Board and the Federal Reserve Bank of New York.

Conclusions and Recommendations

National and international wholesale electronic funds transfers, and messages resulting in such transfers, are accomplished through the FEDWIRE, CHIPS, and S.W.I.F.T. systems. The banking community has grown to rely on these systems as critical channels for the efficient and safe execution of financial and other business transactions. However, the results of our review of the security measures in place to protect these systems from misuse have not been satisfying. The control and management weaknesses we found place these systems at a higher risk than their importance would suggest is acceptable. The nature and extent of oversight of these systems has also varied significantly and the banking agencies' authority over the CHIPS and S.W.I.F.T. systems is uncertain.

Although officials who manage FEDWIRE, CHIPS, and S.W.I.F.T. have generally taken or are taking actions to correct identified weaknesses, oversight needs to be strengthened to ensure the integrity of these systems that are so critical to the smooth functioning of national and international electronic funds transfers.

The operations and security of the FEDWIRE and CHIPS systems are being regularly evaluated by the banking agencies and we believe such oversight activities are essential elements towards ensuring efficient, safe, and reliable services. However, given each system's importance and the extent of control weaknesses we found during our review, we believe that such oversight efforts should be intensified. For example, neither system has had the benefit of full scope external reviews designed to assess system security controls and to render opinions on their reasonableness. We believe that such reviews would help to ensure that these systems have stringent internal controls and that the controls are in place and operating as intended.

The banking agencies have never regulated or examined the S.W.I.F.T. system and such oversight would be complicated since the organization is headquartered in Belgium and the majority of the members of the system are foreign banks whose foreign offices are not subject to examination by United States bank regulatory agencies. While complicated, this system transfers essential messages that form the basis for payment transactions within the United States, and as such, plays an important role in ensuring the safety and soundness of our banking system. Given the internal control weaknesses and other concerns identified in this report, we believe efforts should be undertaken to enhance the oversight and regulation of the system. We also do not share the position of S.W.I.F.T. management that use of external auditors mitigates the need for

an independent internal audit function, and we encourage the organization to establish such a function.

We therefore recommend that:

- The Federal Reserve Board (1) ensure that FEDWIRE control weaknesses identified in appendix II in this report have been satisfactorily corrected; (2) determine whether similar weaknesses exist at other Federal Reserve banks and correct those found; and (3) require annual external reviews of FEDWIRE to help ensure that the system maintains reliable and secure operations.
- The Federal Reserve Board, the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation should exercise their existing authorities to ensure the effectiveness of actions taken by the New York Clearing House Association to (1) develop procedures for the separation of duties for testing, approving, and installing new computer programs, (2) establish and maintain a reporting structure that allows for an independent internal audit function, and (3) utilize external auditors on an annual basis to provide for more comprehensive audit coverage of CHIPS.
- The Federal Reserve Board should work with other central banks and bank supervisory authorities through, for example, the Bank for International Settlements to ensure effective oversight and regulation of the S.W.I.F.T. system and similar systems that serve the international banking community.

We discussed the contents of this report with senior officials of the Federal Reserve System, the New York Clearing House Association, and the Society for Worldwide Interbank Financial Telecommunication S.C. and have incorporated their views where appropriate. In accordance with 31 U.S.C. 718(a), the Federal Reserve System requested an opportunity to officially comment on this report. Its comments are included in appendix III.

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 IV.

Sincerely yours,

A handwritten signature in black ink, appearing to read "Ralph V. Carlone". The signature is written in a cursive style with a large initial "R".

Ralph V. Carlone
Assistant Comptroller General

Contents

Letter	1
Appendix I Objectives, Scope, and Methodology	18
Appendix II Security Weaknesses Identified at Four Federal Reserve Banks	21
Appendix III Comments From the Federal Reserve System	30
Appendix IV Major Contributors to This Report	39
Table	5

Table 1: Control Weaknesses Identified at Federal Reserve Banks

Abbreviations

CHIPS	Clearing House Interbank Payments System
FEDWIRE	Federal Reserve Communications System
GAO	General Accounting Office
IMTEC	Information Management and Technology Division
S.W.I.F.T.	Society for Worldwide Interbank Financial Telecommunication S.C.

Objectives, Scope, and Methodology

Our objectives were to provide information on (1) the reasonableness of security measures in place to help prevent illegal acts against the FEDWIRE, CHIPS, and S.W.I.F.T. systems, and (2) the existing regulatory and legal framework under which these systems are operated and monitored. As agreed with your office, we did not review the level of security provided by depository institutions over the operation of their terminals connected to these systems.

To provide information on the reasonableness of security measures in place to help prevent illegal acts against these systems, we conducted risk assessments of the FEDWIRE, CHIPS, and S.W.I.F.T. systems. Our assessment of FEDWIRE was conducted at the Federal Reserve Board, and the Federal Reserve banks of New York, Chicago, Dallas, and San Francisco. These Federal Reserve banks were selected because they had critical network management, application software development, and systemwide security responsibilities. In addition, these Federal Reserve banks were responsible for processing about 70 percent of the dollar value of electronic funds transfers over FEDWIRE in calendar year 1988. Our assessment of CHIPS was conducted at its data center in New York City. Our S.W.I.F.T. assessment was conducted at the organization's headquarters in LaHulpe, Belgium, and an operating center in the Netherlands.

The risk assessments at these organizations included a review of the susceptibility of the organizations to loss or unauthorized use of system resources, errors in information, and illegal or unethical acts. The risk assessments addressed 16 organizational functions considered to be essential to the secure processing of electronic funds transfers. The functions were (1) security software management, (2) hardware and software management, (3) capacity planning, (4) contingency planning and testing, (5) computer operations, (6) message security, (7) system software management, (8) communications management, (9) network management, (10) quality assurance, (11) data security administration, (12) security awareness, (13) physical security, (14) personnel hiring practices, (15) wire room operations, and (16) internal and external audit reviews. This risk assessment document incorporated questions and control tests from GAO's Control and Risk Evaluation audit methodology, federal standards and guidance within Federal Information Processing Standards Publications of the National Institute of Standards and Technology, and related audit guidelines provided by the Federal

Financial Institutions Examination Council, the Federal Reserve Board, and the American Bankers Association.¹

To document the existing regulatory and legal framework under which these systems are operated and monitored, we reviewed pertinent documentation on the responsibilities, power, and authority of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency. We also obtained federal regulations and other related information from officials in each of the organizations and documented actions taken by the organizations to provide regulatory oversight over FEDWIRE and CHIPS. This included obtaining legal opinions from the General Counsels of the Federal Reserve Board, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency on their legal authority to regulate and examine the CHIPS and S.W.I.F.T. systems. We also reviewed pertinent sections of the Bank Service Corporation Act of 1962 as amended (12 U.S.C. (1867)), which describes federal regulatory oversight responsibilities over bank service corporations.

We also obtained information from senior officials within each organization on whether fraudulent acts have been reported against the FEDWIRE, CHIPS, and S.W.I.F.T. telecommunications systems. In addition, we interviewed senior officials and analyzed data provided by the Federal Bureau of Investigation, Department of Justice, U.S. Secret Service, Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency. Specifically, this review documented whether fraudulent acts were committed by employees within the Federal Reserve System, the New York Clearing House Association, and the Society for Worldwide Interbank Financial Telecommunication S.C. We attempted to obtain information on the number of reported instances of wholesale electronic funds transfer crimes committed by employees or customers of financial institutions that use the FEDWIRE, CHIPS, and S.W.I.F.T. systems. However, information of this nature was not specifically available from law enforcement organizations.

The Society for Worldwide Interbank Financial Telecommunication S.C. limited our access privileges to their operations. In this regard, we were able to discuss technical security features of the S.W.I.F.T. systems with

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 Systems, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, Federal Home Loan Bank Board, and the National Credit Union Administration.

representatives of the organization's Office of Chief Inspector, and reviewed available audit reports prepared by this organization. However, we were not granted access to systems programmers, quality assurance operations, capacity planning staff, contingency planning staff, system software management practices, or external auditors retained by the Society. In addition, we were not able to assess the security afforded to the S.W.I.F.T. operations center located in the United States and we were not provided access to details of the design, development, and testing of the replacement S.W.I.F.T. system.

Except for the access limitations imposed by the Society for Worldwide Interbank Financial Telecommunication S.C., our work was performed in accordance with generally accepted government auditing standards and was conducted between February 1989 and October 1989.

Security Weaknesses Identified at Four Federal Reserve Banks

At the Federal Reserve banks in Chicago, Dallas, New York, and San Francisco we found security weaknesses that increase the vulnerability associated with FEDWIRE electronic funds transfers. We identified 17 security weaknesses in 10 functional areas at these banks. In most cases, each of the Federal Reserve banks have moved swiftly to correct identified security weaknesses. Details of each security weakness and the status of corrective action follows.

1. Software Management Security Weakness: The software that restricts access to FEDWIRE is not properly controlled.

At the four Federal Reserve banks, the system software that restricts access to FEDWIRE was improperly controlled. Specifically, the software was received, tested, modified, and installed on the FEDWIRE system by systems programmers. The Federal Reserve's Data Security Manual states that the data security administration groups at Federal Reserve banks should be responsible for the administration of the security software.

Use of systems programmers to control the receipt and installation of FEDWIRE's access control software instead of data security administration groups reduces the level of control over this software in that systems programmers could, with less chance of detection, make unauthorized software changes. Such changes could cause damage or allow unauthorized access to sensitive information and could result in the destruction of data or the disruption of services.

As a result of this observation, senior officials at the four Federal Reserve banks told us that they have taken steps to strengthen the controls over the administration of the security software. In addition, the Federal Reserve Board incorporated within its financial examination procedures a requirement to determine the adequacy of controls over the installation and use of the FEDWIRE's security software program on a systemwide basis.

2. Physical Security Weakness: Inadequate physical security controls reduce the level of protection afforded critical information and equipment.

A. At the Federal Reserve Bank of Dallas physical security practices were weakened because:

- Critical areas of the data center were not well controlled. Specifically, video cameras or motion sensors were not installed in unmanned areas of the computer center that contained critical computer equipment, including devices that allow direct access to stored data and a communications processor that links the Bank to the Federal Reserve Communications System. This increases the data center's vulnerability to undetected access and destruction of critical equipment.
- Communications lines that link the Bank to the Federal Reserve Communications System are exposed on a wall in the computer center. This increases the vulnerability to data communications disruptions.
- The computer room card key lock system that controls access to and from the facility was inoperable and permitted individuals to exit the room without insertion of their card keys. This weakens the ability of staff to monitor computer center activities.
- Federal Reserve bank guards cannot visually monitor access into the computer center's tape library. A camera in that room is focused on tape drive equipment rather than on the entrance to the room. As a result, a person could enter the tape library and cause damage or remove tapes without being detected.

B. At the Federal Reserve Bank of San Francisco, physical security practices were weakened because:

- There were no cameras or motion detectors in the computer center or in adjoining rooms that contain critical equipment such as the processor that connects the Bank with the Federal Reserve Communications System. This increases the data center's vulnerability to undetected access and destruction of critical equipment.
- An alternate master console that could be used to access the FEDWIRE was located in an unmanned area in the computer room. This increases the risk of destruction of data or disruption of services.
- Access to the computer equipment was not well controlled in that vendors, systems programmers, and others were authorized to access the computer room. In addition, multiple rooms were connected to the center and access to and from these rooms was uncontrolled. These weaknesses hamper the monitoring of computer center staff activities.

C. At the Federal Reserve Bank of New York, we observed the lack of cameras in the data center to monitor unmanned areas that contain critical equipment. The lack of cameras raises the risk to the data center of undetected access and destruction of critical equipment.

**Appendix II
Security Weaknesses Identified at Four
Federal Reserve Banks**

Federal guidance suggests that there should be adequate physical protection and access control to critical data processing areas including the computer room, data control and conversion area, and data file storage area.

Senior Federal Reserve Bank of Dallas officials informed us that they have re-positioned a camera located in the tape library so that entry to and exiting from the library is visible to guards. They also are replacing the card key access system. Bank officials also plan to promptly install additional cameras in unmanned areas of the computer room and enclose the exposed communications lines.

Senior Federal Reserve Bank of San Francisco officials informed us that they are taking steps to place cameras within the computer center. The alternate master console was removed from the computer room. In addition, the Bank has initiated a review of the personnel who have access privileges to the computer center and plan to take appropriate actions.

Senior Federal Reserve Bank of New York officials informed us that the Bank had budgeted for the additional cameras prior to our visit and that they have now been installed.

3a. Computer Operations Security Weakness: FEDWIRE processing can be disrupted because there is no provision for alternate back-up electrical power.

The Federal Reserve Bank of Dallas did not have a generator to provide back-up power during long-term power outages. In addition, it did not have back-up power capability to (1) maintain operations during short-term outages and (2) reduce the adverse effects of power fluctuations. The Bank experienced two power outages during 1988 that disrupted FEDWIRE operations for periods exceeding 30 minutes.

The Federal Reserve's Data Security Manual requires each Federal Reserve bank to have a generating unit of sufficient capacity to support critical operating functions during times of power outages. The manual also suggests that banks obtain a short-term power supply.

The lack of back-up power places the Federal Reserve Bank of Dallas at the risk of not being able to continue critical operations during power outages. Senior Federal Reserve Bank of Dallas officials had budgeted for a system prior to our review and have installed a system that reduces the risk of short-term power outages and electrical surges. In

addition, the Bank plans to purchase and install a generating unit in 1990.

3b. Computer Operations Security Weakness: Controls over the number and type of personnel who have access to FEDWIRE are weak.

A November 1988 Federal Reserve Board financial examination disclosed that 87 San Francisco Federal Reserve Bank employees had access to critical FEDWIRE computer commands and recommended that the Bank reduce the number of individuals with these access privileges. Although the bank responded to the Board's examination, we found that the Bank continued to authorize 48 individuals, including 10 systems programmers, access to critical commands. In addition, we found that master console commands could be issued from multiple computer terminals located outside of the computer room.

The Federal Reserve's Data Security Manual states that authorization to access critical computer commands should be limited to computer operators. The manual also suggests that master console commands should be restricted to one master computer terminal.

Because the Federal Reserve Bank of San Francisco did not adequately restrict the (1) number of personnel with authorization to access critical computer commands and (2) master console commands to one computer terminal, the Bank was more vulnerable to unauthorized data modification and disruption of services.

Senior Federal Reserve Bank of San Francisco officials agreed with our observations and have reduced access to the system from 48 individuals to only nine computer operators. The officials also have taken steps to correct the master console command weakness.

4a. System Software Security Weakness: Changes to software that controls and operates FEDWIRE are not examined from a security perspective.¹

¹System software consists of a set of programs including the operating system, its associated utilities and program products, that allows a computer system to manage its own resources.

Neither the data security administration group nor any other group at the Federal Reserve Bank of New York reviewed the security implications of changes to system software. The Federal Reserve's Data Security Manual assigns responsibility for reviewing the security implications of system software changes to the data security administration group.

Since no review was being conducted, the FEDWIRE system was more vulnerable to, among other things, unauthorized use of or access to electronic data processing resources.

Senior Federal Reserve Bank of New York officials informed us that the Bank's security control group will review new system software changes to determine whether the software changes could create vulnerabilities to FEDWIRE's operating environment.

4b. System Software Security Weakness: Access to software that monitors and operates FEDWIRE was not properly restricted.

The Federal Reserve Bank of San Francisco did not properly restrict access to system software, in that a systems programmer and the data security administrator had the same level of access and privileges to (1) advanced features of online/real-time system performance monitoring software and (2) FEDWIRE's security software.

In order to provide for the segregation of duties between systems programmers and the data security administrator, no systems programmer should be authorized to independently access advanced features of online/real-time system performance monitoring software. As a result of the segregation of duties weakness, the programmer has the capability to allow unauthorized access and changes to sensitive FEDWIRE information without detection.

Senior Federal Reserve Bank of San Francisco officials told us that they have corrected this situation by (1) removing the systems programmers' access privilege to FEDWIRE's security control software, and (2) implementing a procedure to control the systems programmers' access to the advanced features of the system performance monitoring software.

5. Capacity Planning Security Weakness: A computer system was operating at levels that could have a negative impact on the timely processing of funds transfers.

The computer system that operates FEDWIRE at the Federal Reserve Bank of Chicago was operating at levels approaching 100 percent of utilization during peak periods. Although, in March 1988, capacity planning staff at the Federal Reserve Bank of Chicago documented utilization levels exceeding 90 percent, the staff did not recommend that Bank management acquire a new system until September 1988.

The Federal Reserve System does not have a formal policy regarding system utilization levels, but a senior Federal Reserve Board official told us that when a Federal Reserve bank's computer system reaches 80 percent utilization, steps should be initiated to upgrade or replace the system.

Operating the system at excessive utilization levels could cause transaction processing delays and computer processing irregularities that could result in service delays or disruptions.

A Federal Reserve Bank of Chicago official told us that a more powerful computer system has been installed that provides a significant increase in the Bank's computer processing capabilities.

6. Contingency Planning Security Weakness: A Federal Reserve bank may not have been able to resume operations efficiently because it stopped testing with its primary back-up site and did not have a current recovery plan.

The Federal Reserve Bank of San Francisco stopped disaster recovery, contingency planning, and testing at the Federal Reserve System's primary back-up location in September 1988 and was relying on a new location for its disaster recovery and contingency planning before this new site became operational. Also, the Bank's disaster recovery manual was not current and did not include all information needed to re-establish service in the event of a long-term system outage.

The Federal Reserve's Data Security Manual states that each Federal Reserve bank must develop a comprehensive and detailed contingency plan that should be reviewed periodically to account for changes in the status of critical applications. Federal guidance also points out that periodic contingency testing and resolution of problems is necessary to ensure that the contingency plan is adequate and personnel are proficient in responding to emergencies.

**Appendix II
Security Weaknesses Identified at Four
Federal Reserve Banks**

By ceasing contingency testing and not maintaining a current contingency manual, the Bank risked not being able to carry out its disaster recovery and contingency plan in a timely manner.

According to senior officials from the Federal Reserve Bank of San Francisco, the new disaster recovery site became operational in September 1989. In addition, the Bank has prepared an updated disaster recovery manual and has resumed full testing at its new disaster recovery site.

7. Quality Assurance Security Weakness: Improper quality assurance testing weakens internal controls.

The Federal Reserve Bank of Dallas did not properly separate duties within its systems development function. Specifically, a systems analyst was performing both software testing and product acceptance functions. While the Bank did have a quality assurance function, it was primarily involved with developing software standards and procedures—not testing software.

The Federal Reserve's Data Security Manual states that software testing and product acceptance functions should be performed by different individuals when possible. In addition, federal guidance suggests that an independent review of software changes be conducted to ensure that the changes do not permit unauthorized modifications.

By using a systems analyst to perform functions normally conducted by quality assurance staff, the risk of unauthorized software modifications is increased.

Federal Reserve Bank of Dallas senior officials informed us that software acceptance testing is now performed by the quality assurance group. In addition, Bank officials stated that its Production Control Group is now used to move all new programs from the test environment to the operating environment.

8. Communications Management Security Weakness: Communications personnel were performing duties normally assigned to computer operations and systems programmers.

Communications personnel at the Federal Reserve Bank of San Francisco, in addition to performing their traditional responsibilities, performed functions usually assigned to systems programmers and

computer operators. For example, communications personnel had control of a software product that allowed them to issue master console commands that control system operations. These responsibilities are normally assigned to computer operators. The communications personnel also had the ability to use a software product that provides online/real-time system performance monitoring and the capability of altering memory. These responsibilities are normally assigned to systems programmers.

According to federal guidance, a separation of duties should exist within computer operations, systems programming, and communications functions. By not properly separating these functions, the Bank does not have in place key checks and balances to protect against unauthorized access and modification of FEDWIRE data.

Bank officials told us that they will examine the alignment of responsibilities between the computer operations and systems programming functions to eliminate the potential for unauthorized access and modification of FEDWIRE data. In addition, we were told that the Bank has re-assigned access so that the communications personnel no longer have access to advanced features of a specialized software product. The Bank does not plan to separate its communications and computer operations functions in the computer room. The Bank's decision to combine these areas was made consistent with the System's efforts to automate computer and network operations. We continue to believe that the blurring of duties performed by the Bank's communications and computer operations personnel increases the Bank's vulnerability to alteration of data and unauthorized access to FEDWIRE.

9. Network Management Security Weakness: Network management weaknesses leave FEDWIRE more vulnerable to service failures.

The Federal Reserve Communications System, which electronically links all Federal Reserve district banks, did not have totally redundant network nodal processors.² We found that while the nodal processors did provide significant inherent backup capabilities, the memory within the processors is not redundant. Without redundant common memory, these nodal processors have a single point of failure and if a nodal processor becomes inoperable the Federal Reserve Communications System runs

²A nodal processor is a device that provides connectivity between Federal Reserve banks and the Federal Reserve Communications System.

**Appendix II
Security Weaknesses Identified at Four
Federal Reserve Banks**

the risk of not being able to transmit electronic funds transfer data between Federal Reserve banks in its traditional secure fashion.

In addition computer center staff performed incompatible duties including responsibilities associated with software development and management of the network. As a result, network management staff had the ability to make changes to sensitive FEDWIRE communications software utilized by the FEDWIRE application. We also observed that System Communications Center staff were not using state-of-the-art monitoring tools to manage the network and it appeared that they were using hard-copy reports to monitor the system rather than information on real-time display terminals. Events such as these can place the Center at a higher risk of not responding in a timely manner to network management emergencies that require expedient actions.

Federal Reserve Bank of Chicago senior officials informed us that (1) all new processors added to the network contain redundant components as well as redundant memory, (2) controls have been put into place to ensure that network management staff cannot make changes to sensitive FEDWIRE information, and (3) real-time terminal displays have been enhanced.

10. Wire Room Operations Security Weakness: Code words used to authorize FEDWIRE transfers were printed and could have been used to initiate a fraudulent funds transfer.

Within the Federal Reserve Bank of New York's wire room, code words were used to verify telephone funds transfer instructions from financial depository institutions. The code words were printed in a hard copy format that increased the capability to compromise their integrity.

In order to prevent fraudulent fund transfers, employees of Federal Reserve banks should not have the ability to view code words. At other Federal Reserve bank locations we found improved controls over code words in that they were stored in an unreadable format within an automated system.

Since code words could be more easily compromised, the Bank was vulnerable to unauthorized disclosure of information that could result in the initiation of a fraudulent funds transfer. Federal Reserve Bank of New York senior officials told us that code words are now being controlled by a computer system.

Comments From the Federal Reserve System



BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM
WASHINGTON, D. C. 20551

ADDRESS OFFICIAL CORRESPONDENCE
TO THE BOARD

November 9, 1989

Mr. Ralph V. Carlone
Assistant Comptroller General
United States General
Accounting Office
Washington D.C. 20548

Dear Mr. Carlone:

The Board of Governors of the Federal Reserve System appreciates the opportunity to comment on the draft report of the General Accounting Office (GAO) titled Electronic Funds Transfer: Oversight of Critical Banking Systems Should Be Strengthened. To support the effort to develop a timely assessment of electronic data security on the Fedwire system, the Board has expedited its review of the GAO's draft report. Our response should be read in the context of a highly abbreviated comment period providing less than two weeks for staff analysis and Board review.

The Board's response to the portions of the GAO's report related to Fedwire is divided into four parts. First, we provide a general overview of the Fedwire data security architecture. Second, we discuss the GAO's specific findings at the four Reserve Banks visited. Third, we address the GAO's recommendation that the Federal Reserve contract to obtain external review of Fedwire security. Finally, we address the GAO's concern regarding the lack of encryption on the "backbone" communications network linking the Reserve Banks and the need for message authentication.

The Federal Reserve is strongly committed to providing the most secure electronic payments services possible. As noted in the GAO's draft report, the system has in place a comprehensive program designed to identify security requirements, develop and implement technical solutions to those requirements, and, finally, to monitor the ongoing effectiveness of security administration. We believe the security architecture for Fedwire is fundamentally sound, and



- 2 -

we also believe that the GAO's findings will further strengthen the safeguards surrounding Fedwire. The Federal Reserve's commitment to data security for Fedwire is reflected by our receptiveness to information and guidance from various sources that may help ensure excellent security. It is in this context that we welcome the GAO's suggestions for improvement to Fedwire security.

Overview of the Fedwire Data Security Architecture

The Federal Reserve System has implemented a comprehensive security architecture designed to provide secure and reliable electronic payment services. This architecture incorporates a wide range of safeguards, including physical security, controlled access to computer systems, and protection of the confidentiality and integrity of data. These controls apply to software implementation, computer operations, network communications, and contingency. The System establishes and documents its control standards in a Data Security Manual containing over 100 safeguards relating to these areas. The GAO's findings need to be considered in the context of the Federal Reserve's overall security architecture and program. A summary of how these controls provide a secure environment for Fedwire is provided below.

The first level of safeguard in place to protect Fedwire includes physical security that limits access to sensitive data and operations areas to those individuals who require access to perform their duties. Guards, card key access devices, and surveillance equipment are used to prevent and detect unauthorized physical access. Moreover, all employees working in sensitive areas undergo extensive background checks. Further, legal agreements with vendors provide for clearance, nondisclosure, and other appropriate security considerations. Reserve Banks have procedures for reporting, tracking, and resolving computer system problems as well as procedures for reporting suspected security violations. Each Reserve Bank has a complete audit trail for attempted breaches of access controls and the Security Administrator investigates any attempted breach. Where relevant, this information is shared among Federal Reserve Banks.

To safeguard the Fedwire system, access control software and code words identify and permit access to authorized users prior to processing any transfer of funds. The Fedwire system acknowledges successful receipt of messages between system components. To protect confidentiality of messages, transmissions between depository institutions and Reserve Banks are encrypted.

Appendix III
Comments From the Federal Reserve System

- 3 -

Additional controls, based on separation of duties, restrict access to sensitive data and programs. For example, each Reserve Bank maintains separate processing environments for test and critical production systems and restricts access to these systems. Extensive change control mechanisms are in place to ensure that only tested and approved application software changes are implemented in the production environment.

The GAO's interest in security extends to capacity planning and contingency processing arrangements. To ensure that adequate capacity is available, Reserve Banks develop annual automation and capacity plans that fit into a long-range planning process.

The Fedwire system also has been designed to provide for local backup of key computing and communications components. Further, to ensure that Fedwire operations continue with minimum disruption, even after a disaster, the Reserve Banks maintain several remote sites and test comprehensive contingency plans at least semi-annually. These plans include relocation of computer operations, as well as data backup procedures to ensure that databases can be reconstructed after an outage. An example of the resiliency of the Fedwire system was the ability of the Federal Reserve Bank of San Francisco to continue full payments operations following the October 17, 1989, earthquake. The Bank operated on emergency power, restored its computer systems in two and one half hours and resumed processing to meet critical nighttime deadlines, and was open and ready for Fedwire business as usual at 9:00 a.m. Eastern Time the following day. Simultaneously, the Reserve Bank's remote processing site was prepared to serve as backup in the event that critical operations could not resume in San Francisco.

A reflection of the effectiveness of regular production and emergency backup arrangements is the high reliability of the Fedwire applications and the "backbone" communications network connecting the Reserve Banks, called FRCS-80. Availability of Fedwire applications during the critical hours of 5:00 p.m. to closing was 99.60 percent for 1988 and 99.79 percent for 1989 through the third quarter. Availability of Fedwire applications for full-day operations was 99.59 percent for 1988 and 99.77 percent for 1989 through the third quarter. The backbone communications network has also performed well. In over seven years of operations, the FRCS-80 network has maintained availability in excess of 99.99 percent. Planning is also underway for the successor network.

- 4 -

Specific Reserve Bank Findings

The GAO has identified a number of specific control weaknesses at the four Reserve Banks where it conducted on-site reviews. In general, these Reserve Banks have either already taken corrective action with respect to these findings or plan to take corrective action in the near future. The Board disagrees with the GAO's position, however, with respect to one of its findings. The draft report indicates that there should be a complete separation of function between computer and network operators. Based on analysis of both the risk potential and emerging industry trends to automate and consolidate computer and network operations, the Board believes that combining these functions has no detrimental effect on security. A leading industry expert that was consulted by staff concurs with this assessment. Staff comments on this and certain other findings are appended to this letter.

The Board is currently taking steps to determine whether control weaknesses similar to those cited by the GAO exist at any other Reserve Banks. If such weaknesses are found at other Reserve Banks, the Board ensures that prompt corrective action will be taken.

External Review of Fedwire Security

The Federal Reserve's security program includes multiple layers of review, both internal and external. Several organizations within the System play an active role in ensuring consistent compliance with the Federal Reserve's security standards. These oversight groups include a national Security Steering Group, comprised of Reserve Bank and Board staff, the Banks' internal auditors, and the Board's Division of Federal Reserve Bank Operations. Each organization addresses a different aspect of the data security program. At the System level, the Security Steering Group manages and coordinates the development and implementation of the data security design and addresses System-level data and communications matters.

The individual Reserve Banks' internal audit staffs participate in the system development life cycle process, regularly reviewing compliance with security procedures and performing audits of operating and data processing areas. The Reserve Banks' General Auditors report directly to the Banks' boards of directors. The internal audit departments at Reserve Banks also assure that corrective actions are taken in response to recommendations made by the Board's review groups.

- 5 -

A critical component of the Federal Reserve's security program is review and oversight by the Board of Governors, through its staff. The Board exercises, by law, general oversight of Reserve Bank activities. To discharge this responsibility, the Board has established a highly qualified operational and technical staff that reviews the Reserve Banks' implementation of System security standards. The Board's staff is institutionally independent of the Reserve Bank management structure, reporting directly to the Board.

The Board's Division of Federal Reserve Bank Operations reviews Reserve Bank security as an integral part of several of its functions. Through its broad scope operations review of the Reserve Banks' data processing functions, the review program monitors compliance with System policies and identifies actual or potential security concerns. Separate operations reviews of the different functional areas of the Reserve Banks, such as the Fedwire funds transfer and book-entry securities transfer operations, also assess the adequacy of the controls in these functions. The Board's financial examiners also review security as an integral part of the annual financial examination process at each Reserve Bank and assess specifically the effectiveness of electronic access controls for operating systems, networks, and application and environmental software. The examiners' focus also includes a review of the adequacy of administrative and managerial controls related to data security awareness training, personal computers, and local area networks.

To augment this multi-layered data security review program, the Board believes it is useful to engage the services of a consultant from time-to-time to assist its staff in assessing security issues. In fact, the System has a history of employing outside technical assistance. The Board retains an independent accounting firm to review annually its operations review and financial examination oversight functions, including oversight of Fedwire security. We agree that the additional insight from outside parties may be helpful in identifying additional security enhancements. Accordingly, the Board will continue to seek outside expertise to enhance its Fedwire security program. We have found that such reviews are most helpful during major systems changes and will seek outside assistance when we believe that the circumstances warrant such input.

- 6 -

Encryption and Message Authentication

The Federal Reserve is taking steps to address the GAO's concerns regarding the risk of unauthorized disclosure and modification of Fedwire transactions during transmission between Federal Reserve Banks. To understand these actions, a brief description of the "backbone" Federal Reserve Communications System (FRCS-80) is in order.

Implemented in 1982, FRCS-80 is a high-speed, dedicated communications network connecting Reserve Banks, the Board, contingency sites, and the U.S. Treasury. FRCS-80 employs packet switching technology, which breaks messages apart during transmission and reassembles them at their destination. Both the high speed of the backbone communications network and the packet switching technology make penetration of the network difficult. Nonetheless, we believe it is important to take steps to secure the network further. Accordingly, in September 1989, the Federal Reserve issued a request for proposal to encrypt the FRCS-80 backbone network. Vendor responses are currently being reviewed and encryption will be implemented in the first half of 1990. The encryption of the FRCS-80 backbone network is in addition to the encryption of transmissions between depository institutions and Federal Reserve Banks, which currently exists.

The draft report also discusses authentication as a measure to enhance message integrity. Message authentication is a process of deriving a code based on the contents of the message and appending the code to the message for later authentication by the authorized receiver using a secret key shared with the originator. While certain features of the Fedwire network, such as the packet switching technology of the backbone network and the encryption of messages between depository institutions and Reserve Banks, protect the confidentiality of payment information and reduce the likelihood that messages could be altered, the Federal Reserve has been reviewing message authentication technology to determine how to best implement this security feature.

The Federal Reserve has determined that any message authentication technique that is adopted must be consistent with American National Standards Institute (ANSI) Standards 9.9 and 9.17. The technique must also be consistent with Treasury Directive 16-02, which requires the authentication of funds transfers transacted between the Reserve Banks and Treasury Financial Centers. Based upon an understanding with Treasury, the message authentication process currently used for funds transfers conducted with Treasury satisfies this directive. Further, the technique should be commercially available to and cost effective for the depository institutions that are part of the Fedwire network.

- 7 -

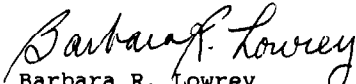
The Reserve Banks are testing the feasibility of implementing message authentication with technology that meets national standards, especially regarding key management, across the Fedwire environment of more than 11,000 endpoints. The feasibility of making message authentication broadly available must account for not only the large number of endpoints but also their diverse size. The majority of the endpoints connected to Fedwire are small depository institutions that are very sensitive to costs. The results and recommendations of the Federal Reserve's feasibility study will be presented to the System's senior management in January 1990. The Board is optimistic that the System's efforts will result in a viable approach to message authentication for Fedwire.

Concluding Remarks

In conclusion, the Board is sympathetic with the thrust of the GAO's recommendations and with a number of its particular findings. Most of the GAO's specific findings have been addressed or are in the process of being addressed. Further, the Board is taking steps to ensure that the conditions leading to the findings do not exist at other Reserve Banks. To enhance its Fedwire security program, the Board will continue to seek outside expertise at times when such assistance would be helpful. The FRCS-80 backbone communications network will be encrypted in the first half of 1990 and recommendations from the message authentication feasibility study will be presented to Federal Reserve senior management in January 1990.

The Board of Governors generally believes that the recommendations contained in the GAO's draft report will assist the Federal Reserve in its continuing efforts to ensure a high level of Fedwire security. We appreciate this opportunity to comment on the draft findings.

Sincerely yours,


Barbara R. Lowrey
Associate Secretary of the Board

Enclosure

- 8 -

ENCLOSURE

DETAILED STAFF COMMENTS ON THE DRAFT GAO REPORT -
ELECTRONIC FUNDS TRANSFER: OVERSIGHT OF CRITICAL BANKING
SYSTEMS SHOULD BE STRENGTHENED

The following discussion addresses areas that the staff believes require further clarification and areas with which the staff takes exception.

8. Communications Management Security Weakness: Communications personnel were performing duties normally assigned to computer operations and systems programmers.

The Federal Reserve Bank of San Francisco does not plan to separate its telecommunications and computer operations functions in the computer room. Operators do not have the ability to modify applications programs or data. The decision to combine these areas was made consistent with the System's efforts to automate computer and network operations. Discussions with an outside consultant with expertise in automated operations have confirmed that there is no additional security risk associated with combining these two functions and that the Bank's decision is consistent with emerging industry trends. However, regarding the GAO's concern about the separation of duties between operations and systems programming, the Bank will reexamine the alignment of responsibilities between these functions to eliminate any potential unauthorized access and modification to Fedwire data.

Further, to address the GAO's concern that the communications personnel had the capability to alter memory, the Bank has reassigned access so that the communications personnel no longer have access to the special password for the software that provides this function.

- 9 -

9. Network Management Security Weakness: Network management weaknesses leave Fedwire more vulnerable to service failures.

The GAO notes that 1) the Federal Reserve Communications network does not have totally redundant backup, 2) computer center staff performed duties associated with software development and management of the network and 3) monitoring of the network appeared to be accomplished by using hard-copy reports rather than using the information on real-time display terminals. Clarification is provided for all these statements.

Regarding the issue of totally redundant backup, all new processors added to the network contain redundant components as well as redundant memory. With respect to the risk of not being able to transmit electronic funds transfer data between Federal Reserve banks if nodal processors become inoperable, the System Communications Center (SCC) maintains back-up equipment that provides recovery for all nodes on the network. In the event of a failure, the backup node is loaded with an image of the failed node software and the site is connected to the back-up node through high speed dial connections. These backup and recovery procedures are tested quarterly with each site and have been used successfully in production when required. The reliability of the network and the adequacy of its backup can be demonstrated by the availability statistics. In over seven years of operations, the FRCS-80 network has maintained an availability in excess of 99.99 percent uptime. In addition, the Federal Reserve System is analyzing alternatives to a successor network.

The GAO notes that the network management staff had the ability to make changes to sensitive Fedwire information. Controls have been put into place to ensure that network management staff cannot make such changes.

Finally, real-time terminal displays are and have always been used to monitor the FRCS-80 network, and recently have been enhanced further. Hardcopy reports are used for archival purposes, not for network monitoring.

Major Contributors to This Report

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

Richard J. Hillman, Assistant Director
William D. Hadesty, Technical Specialist
Gregory P. Carroll, Evaluator

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

Raymond J. Wyrsh, Senior Attorney

**New York Regional
Office**

Bernard D. Rashes, Evaluator-in-Charge
Richard G. Schlitt, Supervisor
Leslie K. Black, Evaluator
David J. Deivert, Evaluator

Requests for copies of GAO reports should be sent to:

**U.S. General Accounting Office
Post Office Box 6015
Gaithersburg, Maryland 20877**

Telephone 202-275-6241

The first five copies of each report are free. Additional copies are \$2.00 each.

There is a 25% discount on orders for 100 or more copies mailed to a single address.

Orders must be prepaid by cash or by check or money order made out to the Superintendent of Documents.

United States
General Accounting Office
Washington, D.C. 20548
Official Business
Penalty for Private Use \$300

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