United States General Accounting Office

GAO

Report to the Chairman, Committee on Science, Space, and Technology, House of Representatives

November 1989

COMPUTER SECURITY

Unauthorized Access to a NASA Scientific Network

GAO/IMTEC-90-2

GAO

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

Information Management and
Technology Division

B-233721

November 13, 1989

The Honorable Robert A. Roe
Chairman, Committee on Science, Space,
and Technology
House of Representatives

Dear Mr. Chairman:

On January 6, 1989, your office requested that we obtain information on instances of unauthorized users gaining access to the Space Physics Analysis Network (SPAN), one of the National Aeronautics and Space Administration's (NASA) unclassified computer networks. As agreed, this report provides (1) a description of SPAN, (2) information on the instances of unauthorized use of the SPAN system, and (3) details on the steps NASA is taking to minimize such unauthorized use.

SPAN was created in 1981 to assist scientists conducting NASA-related research. It provides a system for scientists to share unclassified data and ideas, and to collaborate on space-related NASA research efforts. SPAN has developed rapidly into an international network serving an estimated 100,000 individual users. SPAN connects government, private industry, and university computers in the United States, and provides connections to Canada, Europe, Japan, Australia, and South America. Individual users can access SPAN in various ways. For example, authorized users from almost anywhere in the world can connect to a computer on SPAN using a home computer and the public telephone system.

Results in Brief

NASA records show that between 1981 and March 1989, unauthorized users successfully gained access dozens of times to SPAN computers and used the network to gain access to other SPAN computers located at NASA and another federal agency. Although NASA officials believe that no data have been altered or destroyed, they recognize that they may not be aware of all past instances of unauthorized entry or the damage that may have resulted. Skillful, unauthorized users could enter and exit a computer without being detected. In such cases and even in those instances where NASA has detected illegal entry, data could have been copied, altered, or destroyed without NASA or anyone else knowing. Apart from any damage to scientific data, NASA has incurred additional costs associated with unauthorized users gaining access to SPAN. Although NASA does not keep track of these costs, NASA has said that

recovery from unauthorized computer access or viruses could cost over $100,000.

NASA officials also told us that in all of the known instances of unauthorized entry, the individuals apparently had no destructive intent. If they had, or if they have in the future, the amount of damage that could be done to scientific data is impossible to estimate.

Because SPAN was designed to facilitate the exchange of scientific information, NASA has to balance the desire for convenience and openness with the need to protect valuable scientific data from unauthorized users. This is not an easy task, especially since the current computer security technology does not permit a network that is totally secure and at the same time facilitates the full and open exchange of information.

While NASA has taken or is in the process of taking some actions in response to the security incidents, they have not performed a security risk analysis for SPAN, which is contrary to federal and agency requirements. In the absence of such an analysis, SPAN management does not know the extent of the network's vulnerabilities or the kinds and level of security precautions that should be taken. For example, until a risk analysis is performed, NASA will not know whether (1) the security guidelines it has developed over the past 2 years adequately address the potential risks associated with unauthorized users gaining access to SPAN, or (2) if it is properly balancing convenience and openness with the need to protect valuable scientific data. Because many of the computers on SPAN are not owned or operated by NASA, the task of securing SPAN is a joint responsibility of NASA and its users with NASA taking the leadership role.

Since 1986 NASA has reported to the President and the Congress that it has a material internal control weakness agencywide in the computer security area. The agency reported, among other things, that deficiencies existed in the conduct of risk assessments on a cyclical basis. While it continues to make progress in implementing corrective action, NASA reported in 1988 that actions were not yet deemed adequate to eliminate the material weakness.

NASA's computer security program manager said that the incidents of unauthorized access to SPAN were one of the major reasons that NASA continued to report a computer security internal control material weakness. Performing a risk analysis for SPAN will represent a critical step that NASA can take towards eliminating its computer security internal

control material weakness. As discussed on page 13, we are recommending that the NASA Administrator ensure that a risk analysis of SPAN is performed and documented. In this regard, NASA should continue to report the computer security area as a material internal control weakness in this year's report to the President and the Congress, and discuss the actions that will be taken to correct the weakness.

In performing our review, we examined pertinent management and technical information provided by NASA. We also held discussions with various NASA officials responsible for agencywide security and program management, Goddard Space Flight Center officials responsible for SPAN management, and Marshall Space Flight Center officials responsible for agencywide administrative network operations, as well as several SPAN managers and users at Marshall. More specific details on our objectives, scope, and methodology can be found in appendix I.

Description of SPAN

SPAN is a worldwide computer network linking computers used by scientists conducting NASA space and earth science research. Worldwide, the estimated total number of computers (NASA calls these nodes) directly connected to SPAN has increased rapidly from three in 1981, when SPAN began operations, to about 6,000 in July 1989. NASA authorizes as SPAN nodes those computers that are owned and operated by space science institutions and others that are affiliated with a NASA research project. SPAN connects government, private industry, and university nodes in the United States, and provides connections to Canada, Europe, Japan, Australia, and South America. SPAN also connects to other unclassified NASA, national, and international networks. Users of thousands of computers on other networks also can access SPAN.

SPAN has five routing centers in the United States and one in Europe. The routing centers are used to move data among the various SPAN nodes on the network. The centers are located at the Goddard Space Flight Center at Greenbelt, Maryland; Marshall Space Flight Center in Huntsville, Alabama; Johnson Space Flight Center in Houston, Texas; Jet Propulsion Laboratory in Pasadena, California; Ames Research Center in Moffett Field, California; and the European Space Center in Darmstadt, West Germany.

Major data centers and user facilities available on SPAN include the National Space Science Data Center, which is responsible for archiving and distributing space and earth science data from NASA spacecraft, and

ERSIN in Frascati, Italy, which is a major data center for the European Space Agency.

Some examples of research conducted using SPAN include: (1) collaboration among scientists in Australia, New Zealand, Chile, and the United States when, in 1987, a supernova star, which was observable only in the southern hemisphere, erupted in space; (2) universities and industry studying the Voyager encounter with the planet Uranus; and (3) planning and conducting experiments flown on Spacelab.

SPAN was not designed or authorized to store or process any classified or sensitive data. However, in response to the Computer Security Act of 1987,[1] NASA designated SPAN as a sensitive system because (1) recovery from unauthorized computer access or viruses could cost over $100,000, and (2) compromises to SPAN security could be embarrassing to NASA. In dealing with SPAN security problems, NASA faces the task of providing easy access to data needed by the scientific community while protecting the network and data bases from unauthorized users—individuals who have not been granted permission to use SPAN. Unauthorized access to the SPAN system may be prosecutable under the Computer Fraud and Abuse Act of 1986 (18 U.S.C. 1030) in certain circumstances, such as the intentional unauthorized access to a computer belonging to an agency or department of the government that is exclusively for the use of the government (18 U.S.C. 1030(a)(3)).

According to figures provided by NASA, SPAN's fiscal year 1989 operating costs will total about $4.1 million. The agency was unable to provide similar costs before that year because SPAN's leased line expenses were not separately reported before 1989.

Management of SPAN

SPAN is managed by the National Space Science Data Center located at NASA's Goddard Space Flight Center in Greenbelt, Maryland. While Goddard authorizes the participation of nodes, it delegates to each node manager the responsibility for approving individual users, for ensuring that individual users implement the security guidelines that are established by Goddard, and for ensuring that the node does not contain classified or sensitive data. For example, managers at the node level are generally responsible for (1) monitoring computer transactions for

[1]The Act provides for improving the security and privacy of sensitive information in federal computer systems. In general, the act, among other things, required that all federal agencies identify which computer systems contained sensitive information and establish a security plan for each computer system with sensitive information.

unauthorized activity, (2) controlling access to the computer through the use of security devices and passwords, and (3) educating users on proper network conduct, procedures, and security.

Consequently, Goddard officials may or may not know the individual users on each SPAN node. Based on Goddard officials' rough estimates, the total number of individual SPAN users at the 6,000 nodes is about 100,000.

Primary responsibility for SPAN rests with a project scientist at Goddard, who is also the Associate Chief for the National Space Science Data Center. This official coordinates science activities and general network use and serves as the focal point for the system. The SPAN security manager reports to the project scientist and is responsible for investigating unusual activities on the network and preparing incident reports. As discussed on page 9, NASA has taken various actions in response to SPAN security incidents. However, no mechanism has been established by Goddard to ensure that the more than 6,000 node managers implement the security guidelines that are established or to ensure that each node does not contain classified or sensitive data.

Incidents of Unauthorized Users Accessing SPAN

Although SPAN began operating in 1981, formal reporting and investigating of computer security incidents were not required by NASA until 1988. Between 1981 and 1988, according to NASA officials, they were aware of two major instances involving unauthorized access to SPAN nodes through the network. An incident reporting system was established in 1988. Subsequently, between January 1988 and March 1989, there were 17 reports relating one or more instances where unauthorized users successfully gained access to SPAN nodes a total of 67 times and in many instances used the network to access other SPAN nodes.

None of the reports of these unauthorized accesses disclosed any instances of damaged or destroyed data on SPAN nodes. However, as a result of the activities of unauthorized users in one instance in 1987, service to authorized users on a NASA headquarters administrative computer was disrupted. NASA officials recognize that they may not be aware of all instances where unauthorized users gained access to SPAN nodes, or of damage that may have resulted, including whether scientific data were copied, altered, damaged, or destroyed.

Incident Reporting System Established

In January 1988, NASA developed draft agencywide guidelines for investigating and reporting security incidents related to NASA's computer resources. The guidelines establish procedures to be followed in reporting these incidents, including reporting security incidents monthly to the computer security program manager at NASA headquarters. The program manager is the focal point and coordinator for NASA-wide computer security. Although the guidelines were still in draft in October 1989, NASA officials stated that field centers began reporting security incidents to NASA headquarters in January 1988 in accordance with these guidelines.

The SPAN security manager investigates incidents that occur on SPAN and reports the results to the Goddard security branch. The Goddard security branch is responsible for reporting monthly to the computer security program manager at NASA headquarters.

Incidents Occurring Before 1988

Since formal incident reports were not required by NASA before 1988, we held discussions with agency officials and relied on media reports to obtain information about incidents before that time. Goddard officials told us that between SPAN's inception in 1981 and 1988 they were aware of two major incidents—one in 1984 and one in 1987—where unauthorized users gained access to SPAN nodes and then used the network to access other SPAN nodes.

In 1984, juveniles living in the Huntsville, Alabama, area gained unauthorized access to four nodes connected to SPAN. Although the incident was investigated by the Federal Bureau of Investigation (FBI), according to a Goddard official and newspaper accounts, the juveniles were not prosecuted because of their ages and the fact that no classified information was involved. Using their home computers and the public telephone system, the juveniles wrote programs that placed telephone calls to numbers found in the Marshall Space Flight Center telephone book, recognized which numbers lead to computers, and then guessed passwords. As a result of lax password management, the juveniles were able to gain unauthorized access to three nodes at Marshall, and then used SPAN to gain unauthorized access to one node at Goddard.

In another instance, a Goddard official stated that between June and August 1987, unauthorized users, by exploiting the same flaw in the operating system of each node, gained access to at least 23 different nodes on SPAN at NASA headquarters and field installations in the United

States. Unauthorized access to one of the 23 nodes resulted in the disruption of service to authorized users of a NASA headquarters administrative computer for 1 hour, and disconnection from SPAN for 4 days.

NASA's Office of Inspector General investigated this incident involving the administrative computer. Its report did not identify the unauthorized individuals, but stated that it appeared that they were members of a West German computer club. We were told that Goddard officials informally assessed the risk resulting from this situation and that the flaw in the operating system has been corrected. This incident is the subject of an ongoing investigation by the FBI. Because of the ongoing investigation, information was not available indicating, among other things, the number of unauthorized users involved, the technical details of the attack, or the resultant adverse impact, if any.

Incidents Occurring in 1988 and 1989

Between January 1988 and March 1989, Goddard filed 27 reports of attempts made by unauthorized individuals to access SPAN nodes. Ten of the 27 reports described unsuccessful attempts, and 17 reports described one or more instances where unauthorized users successfully gained access to nodes on the network.

Our analysis of Goddard's 17 reports show that from January 1988 to March 1989 unauthorized users successfully accessed SPAN nodes a total of 67 times and in many cases used the network to access other SPAN nodes. Goddard could not determine the identity of any of the unauthorized users. However, because of patterns in the methods used to gain unauthorized entry, Goddard officials believe that three individuals were responsible for 45 (67 percent) of the 67 unauthorized entries.

One of the three, an individual whom Goddard believes resides in New Jersey, accessed two SPAN nodes at Goddard and one at the Department of Commerce 26 times between March and May 1988. In one instance, this individual gained unauthorized access to a Goddard node from a commercial network, and then used SPAN to access the Department of Commerce node. In another instance, the individual first dialed into Goddard's private branch exchange,[2] gained unauthorized access to a Goddard node, and again used SPAN to access the Department of Commerce node.

[2]Private branch exchange (PBX) systems are, conceptually, miniature versions of telephone company central offices located on the owner's premises. Goddard's PBX is a computerized switching facility that services both voice and data.

In several of these instances, this individual gained unauthorized privileges to two Goddard nodes by using a feature called captive accounts. Captive accounts are intended to provide authorized users with a convenient means to use basic information services such as directories, electronic mail, and newsletters, but prohibit users from exercising greater privileges such as accessing other nodes on SPAN. Access to captive accounts is often made especially convenient by having no password for the account. This individual accessed three captive accounts on two Goddard nodes, and then, because of weaknesses in the controls of captive accounts, used SPAN to gain unauthorized access to the Department of Commerce node nine times. This individual was also able to gain unauthorized access to a Goddard node from a commercial network by guessing the simple password protecting a user account. From the user account, the individual used SPAN to access the Department of Commerce node.

Using a similar approach, a second individual, whose location and identity is unknown to Goddard officials, gained unauthorized access to a total of three nodes at Goddard, the Smithsonian Astrophysical Observatory in Cambridge, Massachusetts, and the University of Miami, 13 times between July and August 1988. This individual gained unauthorized access to a captive account on a Goddard node that was also accessed by the individual from New Jersey, and used SPAN to access the Smithsonian node on three separate occasions.

A third unauthorized user, whom Goddard believes probably was located in Australia, gained access to one node at Goddard and one node at Marshall six times between January 1988 and March 1988. The individual gained unauthorized access to the node at Marshall from a commercial network, and then used SPAN to access the node at Goddard. The Goddard node was vulnerable because it maintained an account that had no password. This account was originally established by the computer manufacturer for use by node managers, and a password was supposed to be implemented for the account once the system became operational. However, the node manager was unaware of the existence of this account, and therefore a password was never implemented for it.

The SPAN security manager was unable to determine the method of access used in the remaining 22 incidents, or to identify the individuals involved or their locations.

Consequences of the Unauthorized Use of SPAN

NASA officials cannot be certain that they have detected all instances of unauthorized access, or that they know all the effects of such access. Skillful, unauthorized users who use valid passwords and prescribed network procedures, or who exploit certain computer operating system flaws could enter and exit a computer without being detected. In such cases and even in those instances where Goddard has detected illegal entry, data could have been copied, altered, or destroyed without Goddard or anyone else knowing. Although Goddard officials believe that no data have been altered or destroyed, they recognize that they may not be aware of all past instances of unauthorized entry or the damage that may have resulted.

Goddard officials also told us that in all of the known instances of unauthorized entry, the individuals apparently had no destructive intent. If they had, or if they have one in the future, the amount of damage that could be done to scientific data would be impossible to estimate.

Apart from any damage to scientific data and disruption of services to users, NASA has incurred additional costs associated with unauthorized users gaining access to SPAN. Although NASA does not keep track of these costs, they include computer and staff time to investigate incidents.

NASA's Response to SPAN Security Incidents

NASA has taken various actions in response to SPAN's security incidents. Some of them have been completed and other actions have been undertaken but not completed. More importantly, NASA has not performed a risk analysis, as required by federal and NASA directives, to ensure its actions—completed and planned—provide adequate security protection for SPAN.

Actions Already Taken

In March 1988, a security specialist already under contract to Goddard was assigned to check weaknesses in the computer operating system, identify methods used to gain unauthorized access to the network, and report these methods and other security weaknesses to SPAN management. The security specialist reports to the SPAN project scientist. Goddard's Associate Director for Programs told us that unauthorized users openly share information such as passwords, operating system flaws and weaknesses, and network addresses through hacker electronic bulletin boards and newsletters. The security specialist monitors these bulletin boards and newsletters and provides SPAN management with information on potential unauthorized user activity.

In February 1989, SPAN management converted a part-time security manager to full time. The security manager's services are provided under an existing contract that provides computer support services to Goddard. The security manager coordinates incident investigations with system managers and with other security organizations both within and outside NASA, reviews computer accounting records for movement of unauthorized users on the network, and evaluates corrective measures for addressing security problems. For example, during one incident the security manager (1) checked computer records to determine when and where the unauthorized user moved on the network, (2) reviewed controls on a captive account that had been breached to determine if the controls had been properly implemented, and (3) contacted a commercial network to determine the unauthorized user's originating network address to block future accesses. The security manager has also provided the FBI with information about unauthorized user activities for its investigations.

Another security weakness that Goddard officials are addressing is the use of easily guessed passwords for user accounts. Goddard has developed a set of software programs (which Goddard refers to as a tool kit) to help node managers provide security for their systems. For example, node managers can use the programs to test user accounts for easily guessed passwords. The programs were completed in May 1989 and are being made available by Goddard officials to node managers upon request. A Goddard official told us that as of July 1989, they distributed 150 sets of the software programs.

Actions Underway but Not Complete

Between 1987 and 1989, Goddard prepared three versions of SPAN security guidelines—one dated January 1987 that was finalized but not widely distributed, and two other versions dated September 1987 and June 1989 that have not yet been made final—to address security problems on the network.[3] The purpose of these guidelines is to inform node managers of the requirements and guidelines that are necessary to maintain an acceptable level of security on the SPAN network.

The January 1987 version, which was general in nature, contains information for detecting computer break-in attempts. The project scientist

[3]In 1985 and 1986, security guidelines were also developed as part of a general SPAN management document, but we were told these guidelines were distributed to only a small number of local managers.

told us that this version received relatively limited distribution electronically over SPAN, by telephone and mail requests, and during user conferences. In September 1987, Goddard updated and expanded the January version by adding detailed security information on the basis of lessons learned as a result of unauthorized users gaining access to SPAN. Among other items, the guidelines discuss security considerations for establishing user accounts, managing passwords, detecting unauthorized access to a computer, and handling a successful unauthorized entry. Distribution of the September 1987 version has been very limited because the project scientist decided it contained information that could be useful to unauthorized users attempting to access the network. Consequently, distribution has been limited to selected individuals, such as routing center managers. Goddard officials stated that the only way these managers can obtain the September 1987 draft is to request it through the project scientist. The project scientist said the September 1987 version of the SPAN security guidelines was not finalized because staff time was not available to remove the sensitive information it contains.

In June 1989, Goddard again revised its September 1987 draft security guidelines. This version contains some information found in the 1987 versions as well as new information resulting from more recent experience. Goddard officials told us they plan to issue the new guidelines in the fall of 1989 to managers at major sites. Goddard also plans to distribute the guidelines at a SPAN user meeting scheduled for the fall of 1989.

These guidelines contain information that could have been useful to node managers had the guidelines been finalized and or more widely disseminated earlier. Incidents have occurred on SPAN since 1987 that were addressed in the guidelines. For example, both the January 1987 and September 1987, as well as the June 1989 versions, contain instructions to assist managers in protecting their nodes if captive accounts are established in their computers. The June 1989 version points out that the manufacturer has made statements to the effect that it is impossible to make a captive account totally secure, and that managers should be very cautious in allowing them on their nodes. On the basis of past incidents of unauthorized accesses related to captive accounts, the guidelines contain a list of procedures and precautions for managers. The guidelines also identify minimum security precautions that node managers should take in managing passwords.

Additional Action Needed

Contrary to federal and NASA requirements, however, Goddard has never done a formal security risk analysis for SPAN. Office of Management and Budget (OMB) Circular A-130 requires federal agencies to perform a risk analysis at least every 5 years to ensure that appropriate, cost effective safeguards are incorporated into existing and new computer installations and networks. The objective of a risk analysis is to assess the vulnerabilities and threats so that the security resources can be effectively deployed to minimize the potential loss. Federal Information Processing Standards Publication 65, Guideline for Automated Data Processing Risk Analysis, also requires agencies to perform risk analyses and identifies two key elements that must be considered: (1) the damage that can result from a breach of security, and (2) the likelihood of such a breach occurring. The publication points out that the aim of a risk analysis is to help management strike an economic balance between the impact of risks and the cost of protective measures.

NASA officials agreed that a risk analysis has not been performed for SPAN. The NASA official responsible for the agency's computer security program stated that instead of attempting to conduct a risk analysis of SPAN itself and its interface to other major international agency networks, NASA is focusing on physical installations. This official said that NASA centers are responsible for conducting risk analyses for hardware, software, and telecommunications network components, including SPAN nodes and telecommunications equipment. However, although requested, NASA was unable to provide us with any documentation showing that such analyses had been performed for SPAN components. Goddard did provide us with three undated safeguard assessments completed for Goddard computers connected to SPAN. These assessments were for SPAN nodes at the National Space Science Data Center, NASA Space and Earth Sciences Computing Center, and the Goddard Image and Information Computer Center. These one- or two-page safeguard assessments were general in nature and focused on physical safeguards. However, the assessments did not analyze the risks of unauthorized users gaining access to nodes at Goddard and using them to gain unauthorized access to SPAN, nor did they address the cost effective measures needed to protect the network.

As discussed below, since 1986 NASA has reported to the President and the Congress that it has a material internal control weakness agency-wide in the computer security area. In this regard, the Federal Managers' Financial Integrity Act of 1982 (31 U.S.C. 3512 (b) and (c)) requires federal department and agency managers to evaluate whether internal control systems have weaknesses that can lead to fraud, waste,

and abuse in government operations. The act is a key mechanism that the Congress has put in place to ensure that management controls, including those over automation efforts, are effective, and to hold managers accountable for correcting identified deficiencies. Federal managers are required to report annually to the President and the Congress on their systems and plans to correct identified weaknesses.

NASA reported to the President and the Congress in December 1986, and each year since then, that its computer security internal controls did not meet the management requirements addressed in OMB Circular A-130 and thus identified its computer security internal controls as a material weakness.[4] During 1986, NASA said it reviewed and analyzed its computer security internal controls and, based on the results, was not reasonably assured of the adequacy of its existing security; therefore, a material weakness was reported. The agency reported, among other things, that deficiencies existed in the conduct of risk assessments on a cyclical basis. While it continues to make progress in implementing corrective action, NASA reported in 1988 that actions were not yet deemed adequate enough to eliminate the material weakness. NASA's computer security program manager said that the incidents of unauthorized access to SPAN were one of the major reasons that NASA continued to report a computer security internal control material weakness.

Recommendation

We recommend that the NASA Administrator ensure that a risk analysis of SPAN is performed and documented. On the basis of this analysis, NASA, in cooperation with the SPAN users, should develop an approach for ensuring that the security measures resulting from the risk analysis are implemented by the SPAN managers and users. In this regard, NASA should continue to report the computer security area as a material internal control weakness in this year's report to the President and the Congress, and discuss the actions that will be taken to correct the weakness.

Agency Comments

NASA provided official oral comments on a draft of this report on October 4, 1989. The NASA official responsible for the agency's computer security program agreed with our findings and that a more formalized

[4]The Office of Management and Budget has defined a material weakness as a specific instance of noncompliance with the Financial Integrity Act of sufficient importance to be reported to the President and the Congress. Such weaknesses would significantly impair the fulfillment of an agency component's mission; deprive the public of needed services; violate statutory or regulatory requirements; significantly weaken safeguards against waste, loss, unauthorized use or misappropriation of funds, property, or other assets; or result in a conflict of interest.

process for conducting and documenting risk assessment activities associated with SPAN is necessary. This official stated that NASA intends to take action to accomplish this. This official also stated that as technology for network risk assessments evolves, NASA intends to continually improve this ongoing risk assessment process.

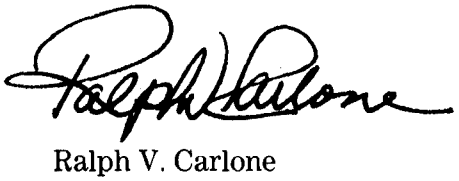
NASA's computer security program manager pointed out that SPAN management has worked closely with one computer manufacturer whose equipment is used extensively on SPAN to obtain security-related software revisions as soon as possible for implementation on NASA-owned computer systems.

NASA's computer security program manager also pointed out that with the addition of a full-time SPAN security manager the agency plans to take more of an aggressive approach to computer security by alerting the SPAN user community to security vulnerabilities and prescribing the precautions that should be taken.

As arranged with your office, unless you publicly release its contents earlier, we plan no distribution of this report until 30 days after the date of this letter. At that time, we will send copies to other appropriate congressional committees; the Administrator, NASA; and other interested parties upon request.

This work was performed under the direction of Samuel W. Bowlin, Director for Defense and Security Information Systems, who can be reached at (202) 275-4649. Other major contributors are listed in appendix II.

Sincerely yours,



Ralph V. Carlone
Assistant Comptroller General

Objectives, Scope, and Methodology

On January 6, 1989, the House Committee on Science, Space, and Technology asked us to report on unauthorized users gaining entry into the National Aeronautics and Space Administration's (NASA) Space Physics Analysis Network (SPAN). Specifically, we agreed to provide (1) a description of SPAN, (2) information on the instances of unauthorized use of the SPAN system, and (3) details on the steps NASA is taking to minimize such unauthorized use.

To obtain information about the unauthorized accesses to SPAN and the steps being taken to minimize the probability of their reoccurrence, we analyzed Goddard Space Flight Center incident reports of unauthorized users gaining access to SPAN for the period January 1988 to March 1989. Since formal reports were not required before 1988, we held discussions with agency officials and relied on media reports about incidents before 1988. We also reviewed a NASA Inspector General report concerning computer security incidents that occurred on SPAN in July and August 1987 at the NASA Headquarters Computer Center.

We also reviewed NASA and SPAN management instructions and guidelines, other NASA documents relating to computer security, Office of Management and Budget guidelines for implementing the Computer Security Act of 1987, and National Institute of Standards and Technology guidance on computer security.

We interviewed officials at NASA headquarters, Goddard Space Flight Center, and Marshall Space Flight Center, as well as NASA contractor staff representing Science Application Research; Boeing Computer Support Services, Incorporated; Booz-Allen and Hamilton, Incorporated; and NYMA Incorporated. We also interviewed a security specialist at George Washington University and the National Institute of Standards and Technology, and six SPAN node managers at Marshall concerning whether they had received written SPAN security guidelines, how familiar they were with security issues, and to what extent they had implemented SPAN security policies and procedures. We conducted our work at NASA headquarters in Washington, D.C.; the Goddard Space Flight Center in Greenbelt, Maryland; and the Marshall Space Flight Center in Huntsville, Alabama.

We obtained official oral NASA comments on our report on October 4, 1989, and incorporated the comments in the report where appropriate. Our review was performed between January and July 1989 in accordance with generally accepted government auditing standards.

Major Contributors to This Report

Information Management and Technology Division, Washington, D.C.	Stephen A. Schwartz, Assistant Director Don J. Ward, Evaluator-in-Charge Scott M. Berger, 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