Office of
INSPECTOR GENERAL

Audit Report

Audit of the USITC Local Area Network Operations

Report No. IG-01-96

UNITED STATES INTERNATIONAL TRADE COMMISSION

March 1996

Date Issued

INSPECTOR GENERAL

UNITED STATES INTERNATIONAL TRADE COMMISSION

WASHINGTON, D.C. 20436

March 15, 1995

REVIEW OF USITC LOCAL AREA NETWORK OPERATIONS

Since 1988, the Commission has invested a substantial amount of resources into automating agency functions and implementing a Local Area Network (LAN) using Banyan Vines that reaches virtually every employee. An audit report issued in September 1992 made numerous recommendations for improving security and procedures. The objectives of this review were to: update the 1992 evaluation of the Commission's administration and control of the LAN; assess the adequacy of LAN security; and evaluate the appropriateness of Commission policies on use of the LAN.

This review was conducted by Cotton & Company in accordance with the Government Auditing Standards issued by the Comptroller General of the United States. The auditors found that the procedures were sufficient, in all material aspects, to provide for effective LAN administration and control, but identified several areas in which controls should be strengthened to remove potential security weaknesses.

The auditors found:

-- Security control weaknesses exist regarding use of modems;

-- Unauthorized and fictitious users are not deleted from the network on a timely basis;

-- Procedures for investigating security violations should be strengthened;

-- A security plan should be developed and security controls tested;

-- Unauthorized persons have access to backup tapes;

-- Procedures for assuring compliance with software licensing requirements are inadequate;

-- Procedures for transporting backup tapes are not documented;

-- The disaster recovery plan is not tested;

-- The titles and roles of network administrators should be clarified; and

-- Policies regarding non-essential software and unofficial computer use should be established.

Recommendations addressing these findings are presented after each section in the report.

The Director of the Office of Information Services concurred with the findings and recommendations. A summary of the Director's comments is presented after each finding on pages 6 through 14. The Director's comments are presented in their entirety as an appendix to the report.

Jane E. Altenhofen

Jane E. Altenhofen
Inspector General

REPORT ON REVIEW OF
UNITED STATES
INTERNATIONAL TRADE COMMISSION
LOCAL AREA NETWORK
OPERATIONS

OCTOBER 1995

Prepared by:

Cotton & Company
Certified Public Accountants
Alexandria, Virginia

CONTENTS

REPORT ON REVIEW OF UNITED STATES INTERNATIONAL TRADE COMMISSION LOCAL AREA NETWORK OPERATIONS

The United States International Trade Commission (ITC) is an independent Federal agency with broad investigative powers on matters of trade. In its adjudicative role, ITC determines injury and threat of injury by imports to United States industry.

ITC has determined that it is more cost effective to use cross-servicing and timesharing agreements rather than to maintain internal mini- or mainframe computer capability. Thus, it obtains general data processing facilities from the National Institutes of Health, financial system support from the Department of Interior, payroll services from the General Services Administration, and personnel management support from the Department of Energy.

Since 1988, however, ITC has invested substantial resources to automate agency functions and implement a local area network (LAN). A LAN is a geographically confined computer-based communications system capable of transmitting information or data among stations. ITC's LAN system is Banyan Vines.

As of September 1995, ITC's LAN consisted of 11 file servers running Banyan Vines 5.5, several special application servers, such as a fax server, and approximately 470 personal computers as workstations.

The LAN supports a variety of office automation functions, including word processing, electronic mail, spreadsheets, and end-user database applications. Software includes Windows, Wordperfect, Lotus 1-2-3, dBase, Harvard Graphics, Timetalk, Electronic Mail (e-mail), and Tackboard. The system contains unclassified as well as sensitive information, such as confidential business information. Users are provided network and computer security training.

As set forth in USITC Directive 1031, dated February 6, 1994, the Office Automation Support Division (currently the Information Services Division), within the Office of Information Services (OIS), is responsible for:

- Central network administration including all LAN connectivity and communication interfaces with computer service bureaus and mainframes, network hardware, software, maintenance, cabling, and user support.

- Office automation technical support including installing, maintaining, and supporting end-user equipment and software and providing end users with supplies and services as needed.

- Implementation of Federal government policies, principles, guidelines, and standards for LAN operations.

- LAN security.

ITC has two primary objectives regarding LAN security. Although it is ITC's policy not to store confidential business information on the LAN, many users process confidential business information on the LAN and remove it once a task is complete. Therefore, confidential business information, while being processed on the LAN or stored on backup tapes, must be protected against security breaches. ITC's second objective is to protect data from being lost or altered, thus resulting in economic loss caused by the need to recreate and reprocess data.

OBJECTIVES

We reviewed ITC's policies and procedures for managing its LAN. Our overall objectives were to update the 1992 evaluation of ITC's administration and control of the LAN, assess the adequacy of LAN security, and evaluate the appropriateness of policies on LAN use. Specific objectives were to:

- Determine if recommendations made in the 1992 Audit Report IG-04-92 and suggested actions agreed upon by management and the Office of Inspector General (OIG) have been implemented and effectively address the findings.

- Determine if LAN security has been compromised, and evaluate computer system controls.

- Determine the existence of unauthorized or unlicensed software on personal computers (PCs) and, if found, determine how programs were installed.

- Evaluate the appropriateness of allowing games, which may be part of authorized or licensed software, to be on ITC equipment.

- Identify the number of system administrators and the extent of their access to the LAN. Determine how they are selected and trained. Determine if their access to the LAN presents an excessive risk and what controls are in place to reduce that risk.

- Identify officials with responsibility for and access to off-site backup data and disaster recovery. Evaluate the backup and recovery system and procedures and disaster recovery plan for compliance with laws and regulations and efficiency.

- Determine which employees can access LAN files (including deleted e-mail messages) other than their own and if a trail is left.

- Evaluate controls established to prevent virus infections and determine compliance.

- Review ITC policy and procedures for using ITC computer equipment for non-official use and evaluate for reasonableness, enforceability, and compliance with laws and regulations.

SCOPE

We conducted our review of ITC's policies and procedures for managing its LAN during August and September 1995 at ITC headquarters in Washington, DC. The review was conducted in accordance with generally accepted Government auditing standards.

METHODOLOGY

In the context of the above objectives, we:

- Interviewed selected ITC officials and reviewed documents to evaluate ITC policies and procedures applicable to LAN administration, control, and security.

- Evaluated existing system controls, tested a sample of PCs to determine the existence of unauthorized or unlicensed software, and looked for evidence of LAN security compromises or violations.

- Identified LAN network and group administrators, the extent of their access to the LAN, and procedures to prevent security risks.

- Examined procedures for backing up the LAN and storing and accessing the backup devices, and interviewed the contractor that stores backup tapes.

- Inquired about ITC's disaster recovery plan and security plan.

- Tested e-mail access to determine if users can access another user's e-mail files and determined if e-mail can be retrieved from backup devices by unauthorized staff.

- Tested and evaluated controls to detect or prevent virus infections on ITC equipment.

- Evaluated the reasonableness and enforceability of ITC policies regarding non-official use of ITC equipment.

- Determined if actions taken to correct previous audit findings had been effectively implemented.

We used the following guidelines and operating regulations to evaluate ITC's LAN administration:

- Federal Information Processing Standards Publication (FIPS PUB) No. 112, Password Usage, dated May 30, 1985.

- Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, effective June 25, 1993.

- Proposed Revision to OMB Circular A-130, Appendix III, Security of Federal Automated Systems (Federal Register, Volume 60, No. 63, dated April 3, 1995).

- OMB Bulletin No. 90-08, Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information, dated July 9, 1990.

- Computer Security Act of 1987, Public Law 100-235 [HR 145], dated January 8, 1988.

- United States General Accounting Office (GAO), *Standards for Internal Controls in the Federal Government*, 1983.

- ITC Guidelines:

  - Directive 1031, OIS, Office Automation Support Division, Mission and Functions Statement, dated February 6, 1994.

  - Directive 1360.1, Automated Data Security Procedures, dated July 21, 1993.

  - Directive 1355, Handling and Safeguarding Confidential Business Information, dated July 1, 1985.

  - Directive 7102.1, Guidelines for using the USITC Local Area Network for Electronic Mail and Bulletin Board Purposes, dated January 8, 1990.

  - Directive 3050, Emergency Recovery Contingency Plan, dated March 8, 1993.

  - Administrative Order 93-01, Adherence to Computer Software Licensing Agreement and Copyright Restrictions, dated October 8, 1992.

  - Banyan Network User's Manual, dated August 1993.

  - OIS' Senior Network Administration Procedures, undated.

MANAGEMENT CONTROLS

In planning and performing our review of ITC's LAN, we assessed ITC's management control structure to the extent deemed necessary to plan and conduct the review and form conclusions related to the review objectives and not to provide assurance on the management control structure.

FINDINGS AND RECOMMENDATIONS

The findings and our recommendations are discussed below.

1. Security Control Weaknesses Exist Regarding Use of Modems

We noted several areas in which controls over the use of modems should be strengthened to remove potential security weaknesses.

- We noted that some network users have stand-alone modems (external and internal) at their workstations. ITC indicated that some modems were provided to dial out to host computers, in part because the modem pool was insufficient to meet peak workloads. ITC does not have an inventory of workstations with stand-alone modems and does not have procedures for controlling and monitoring their usage.

  ITC Directive 1360.1, Chapter I, Procedures for Remote Dial-Up Access, states that users connecting to the LAN remotely must use the central dial-up facility and may not dial the personal computer in their office.

  However, OIS is aware of instances in which users did not logout or turn off their computers after business hours. It is possible that users could remain logged into the LAN and simultaneously leave communications software running in the "answer" configuration thus enhancing the risk of unauthorized access to the LAN.

- ITC has one modem in the modem pool that is set to accept incoming calls without confirming the user's authenticity through the dial-back feature. This modem was established to permit users on travel status to access e-mail only. In order to access this modem, the user must be running Banyan Vines software on the remote PC and have an account with a valid name and password combination. While these controls will help prevent security violations, we noted that ITC does not currently log users of this modem or maintain active and up-to-date lists of authorized users. Without user logs and regular monitoring of activity, ITC cannot detect and investigate potential or actual access by unauthorized users.

  OMB Circular A-130, Section 8.a(1)(g), Policy - Information Management Planning, states that agencies shall protect government information commensurate with the risk and magnitude of harm that could result from the loss, misuse or unauthorized access to or modification of such information.

- In response to a prior audit report recommendation, ITC established a dial-in modem pool with a dial-back control feature and implemented controls to monitor access authorization and actual activity. We noted, however, that OIS does not periodically prepare and distribute to office directors and supervisors reports identifying authorized users and actual activity. Because the dial-in facility is intended only for those having a specific need to access the network from an authorized remote location, periodic review by office directors and supervisors will help assure that access is limited to persons needing access and that abuse does not take place.

The GAO *Standards for Internal Controls in the Federal Government*, Specific Standard No. 5, Supervision, states that qualified and continuous supervision is to be provided to ensure that internal control objectives are achieved.

Recommendations. We recommend that the Director of OIS:

a. Determine the number and location of stand-alone modems not included in the modem pool and their usage rate; retrieve all external and internal modems; and determine if the modem pool should be increased to meet peak workloads. If OIS maintains that stand-alone modems are justified, establish special controls, such as a dial-back feature or limited hours of access.

b. Prepare and update a report that identifies who has access to the modem without the dial-back feature and when authorization was granted and deleted.

c. Establish procedures to identify and monitor the activity of the modem without the dial-back control feature that will enable OIS to detect and investigate unauthorized access.

d. Circulate reports identifying authorized users of the modem pool and activity reports showing usage of the modems to office directors and supervisors on a periodic basis to assure that users are granted access only when necessary and that users are not abusing their access rights.

Commission Response. OIS stated that the security threat resulting from unauthorized modem use is minimal and the cost and inconvenience of implementing additional reports and restrictions are not justified. It did agree, however, to implement closer monitoring of failed login attempts via the non-dial-back modem since doing so will not involve extensive administrator time.

The General Counsel stated that the recommendation regarding limited hours of access to the LAN would interfere significantly with legitimate agency business because employees work late hours and on weekends.

Auditors' Additional Comments. We agree that the proposed action will help identify possible or actual instances of unauthorized LAN access. If incidents are identified, we think that OIS should implement our other recommendations.

2. Unauthorized and Fictitious Users Are Not Deleted from the Network on a Timely Basis

ITC does not have procedures in place to assure that user identifications (IDs) are deleted on a timely basis when employees are terminated or transferred within ITC. We noted that terminated and transferred employees, including network administrators, remained on the LAN user access list after termination or transfer dates. OIS indicated that if an employee's user ID was not deleted, in which case the employee remains on the access list, the employee will not have access to the LAN if his or her password was changed, or disabled. OIS cannot, however, produce a report that shows if or when passwords are changed, or disabled.

Based on discussions with various ITC representatives, and review of Directive 1360.1, system administrators or coordinators (Group Administrators) are responsible for deleting user IDs or requesting OIS to delete them when employees leave ITC or are transferred within ITC. OIS does not have procedures to assure that this is being done in a timely manner. Accordingly, access to the LAN may be granted to unauthorized personnel. OIS is responsible for LAN security and thus should assure that unauthorized users and user accounts are deleted from the system in a timely manner.

We also noted several fictitious user IDs on the LAN. ITC does not have a policy or guidelines for creating, using, and deleting fictitious user IDs. Accordingly, a fictitious user ID may be created inappropriately or remain longer than necessary or after the person who created it leaves ITC, thus increasing the risk of unauthorized LAN access.

ITC Directive 1360.1, Section 4, Responsibilities, states that the Director of OIS is responsible for administering the assignment and maintenance of user IDs and passwords for the LAN access including clearance of all departing ITC staff who have been assigned passwords.

Recommendations. We recommend that the Director of OIS:

a. Establish procedures to assure that Group Administrators have deleted user IDs for all terminated and transferred employees on or before the individual's last workday or date of transfer.

b. Establish and document policies and procedures to minimize the creation and use of fictitious user IDs and to assure that they are deleted as soon as they are no longer needed or before an employee using the fictitious ID leaves ITC.

Commission Response. OIS stated that OIS has a procedure in place to verify that departing employees are deleted from the network, although it involves a delay of up to one month from the date the employee departs. OIS believes, however, that the security threat from departing employees is small, and stated that it has not become aware of any actual or suspected threat of compromise or destruction of data by departing employees.

OIS stated that it will, however, implement an annual review of fictitious accounts to establish the continuing need for each or to delete them.

Auditors' Additional Comments. OIS procedures for verifying that departing employees are deleted from the LAN appear adequate if Group Administrators are, in fact, deleting departing employee IDs on or near their departure date. If OIS determines that Group Administrators are not deleting departing employee IDs in a timely manner, OIS should either review and strengthen the Group Administrator procedures or revise its procedures for assuring that IDs are deleted as soon as employees depart the Agency.

3. Procedures for Investigating Security Violations Should Be Strengthened

OIS should strengthen current procedures for reviewing possible or actual security violations. An OIS representative stated that ITC does not regularly log all network activities, but rather has set the system log to record only login and logout activities to minimize the use of network resources. Such logs are only casually examined for potential security threats.

OIS represented that it reviews the system log on the server for failed login attempts and discusses them with the user. OIS does not, however, produce an exception report of failed login attempts or document the results of its review of the system log.

If a large number of bonafide login failures exists, and an exception report is not produced, a true security violation may go undetected. In addition, if exception reports are produced, OIS will be able to analyze login failures for patterns and thus minimize the number of failures or more easily detect security violations.

OIS' Senior Network Administration Procedures, Section 1.A, System Performance/Security Logs, states that the senior network administrator must maintain a weekly "Network Log" which includes the token ring address of any individual who attempts to log into the network unsuccessfully more than three times. Currently, OIS is not including this on its weekly Network Log.

Recommendations. We recommend that the Director of OIS:

a. Obtain software to produce an exception report from the system logs identifying actual or possible security violations.

b. Establish procedures to investigate and resolve all possible security violations and document such resolution on the exception log for review by the appointed LAN security officer.

Commission Response. OIS stated that the additional time and cost needed to investigate and resolve all possible security violations would greatly outweigh the small amount of additional security provided by implementing the audit recommendations. OIS will, however, re-establish the procedure of recording the network hardware ("token ring") location of unsuccessful logins on the weekly Network Log.

Auditors' Additional Comments. If OIS does not produce an exception report, OIS should, at a minimum:

- Continue to review the system log for failed logins.
- Discuss all failed login attempts with the LAN users.
- Include the token ring address for failed logins on its weekly Network Log.

4. Security Plan Should Be Developed and Security Controls Tested

OIS representatives indicated that ITC does not have a documented security plan. We noted several practices established by OIS that increase the risk of security violations.

- LAN users have 24-hour 7-day-per-week access to the LAN. OIS indicated that it has observed that users sometimes leave their computers logged or powered on during evenings or weekends. If users had limited access to the LAN, OIS could set the system to automatically logoff users that did not logoff before leaving work.

- LAN users can logon to more than one workstation simultaneously. If a user logs on to a workstation other than his or her own and does not subsequently log off, another employee could access the files of the first user without proper authorization.

- One network administrator account is shared by five network administrators using the same password. OIS indicated that this account is used to perform backup functions, which are accomplished by any of the network administrators and generally require more than one administrator to complete. In the event that a backup is made for an unauthorized purpose, by a user of the shared account, OIS may not be able to detect who conducted the unauthorized activity.

OIS representatives indicated that the security risks associated with each of the above practices have been considered and minimized by compensating controls. OIS should, however, have a documented security plan that addresses ITC's consideration of each of the Banyan Vines Network security options, identifies controls in place to minimize possible violations, and states the installation standards adopted by ITC.

OMB plans to implement proposed revisions to OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems, in the near future. This proposed revision will replace OMB Bulletin 90-08. The proposed revisions require the development of security plans that include specific security controls and periodic review of these controls.

Recommendations. We recommend that the Director of OIS:

a. Develop a security plan that complies with the requirements of the proposed revisions to OMB Circular A-130, Appendix III, and that addresses ITC's consideration of each of the Banyan Vines Network security options, identifies controls in place to minimize possible violations, and states the installation standards adopted by ITC.

b. Establish a plan for reviewing security controls and assure that it is implemented in accordance with the requirements of the proposed revisions to OMB Circular A-130, Appendix III.

Commission Response. OIS stated that it will develop a security plan that conforms to the draft revised guidance in OMB Circular A-130.

5. Unauthorized Persons Have Access to Backup Tapes

OIS staff other than the network administrators have access to both daily and weekly backup tapes. We noted that several OIS employees other than the network administrators had access to the computer room and the combination to the containers in which the weekly backup tapes are kept. The daily back-up tapes are kept in the computer room but not locked in containers. This increases the risk that network data, including confidential business data, may be obtained by unauthorized persons.

In addition, the backup tapes are not erased or de-gaussed after they are returned from off-site storage. OIS indicated that it backs up data for the current week on old backup tapes. If data for the current week are not sufficient to copy over all data on the tape, the old data remain on the tape. In the event the tapes are lost or stolen, ITC may not be able to ascertain the actual data lost.

OMB Circular A-130, Section 8.a(1)(g), states that agencies shall protect government information commensurate with the risk and magnitude of harm that could result from the loss, misuse or unauthorized access to or modification of such information.

Recommendation. We recommend that the Director of OIS modify its procedures to require both daily and weekly backup tapes to be safeguarded from unauthorized access by other than network administrators, and erased or de-gaussed after they are returned from off-site storage.

Commission Response. OIS stated that it will maintain a lockbox in the computer room for the storage of backup tapes.

Auditors' Additional Comments. We continue to think that erasing or de-gaussing the backup tapes is necessary to identify compromised data in the event the tapes are lost or stolen.

6. Procedures for Assuring Compliance with Software Licensing Requirements Are Inadequate

ITC does not have adequate procedures to assure that it does not violate software copyright restrictions. In response to a prior audit report recommendation, ITC began maintaining an inventory list of software purchased by ITC. This list does not, however, include software installed by computer vendors and does not indicate the total number of licenses owned by ITC for each software program, including network software. The list also does not indicate on which computer the software is installed and how many licenses are available for other users. Therefore, ITC cannot readily determine the number of licenses it owns and the number available for other users.

In addition, ITC does not maintain a record of what software is loaded on each PC and compare this record to its inventory list. Accordingly, ITC cannot readily detect copyright violations. Neither OIS nor employees could produce proper licenses for some software installed on PCs.

U.S. Code, Title 17, Copyrights, states that anyone who violates any of the exclusive rights of a copyright owner is an infringer of the copyright and is subject to action taken by the copyright owner. ITC Administrative Order 93-01 states that ITC employees are prohibited from violating copyright laws.

An ITC representative indicated that many software packages are "self-metering," and that ITC also obtains site licensing to assist in preventing copyright problems. Self-metering only works, however, on network software. If network software is copied to a PC, the self-metering control will not work. In addition, ITC purchased many stand-alone copies of software programs, which should be monitored to assure that the licensing agreements are not violated.

Recommendations. We recommend that the Director of OIS:

a. Update its software inventory list to ensure that it contains all software for which ITC has a license, including software loaded on computers when purchased.

b. Sort the inventory list by software program and total the number of licenses for each software program.

c. Identify all software installed on each computer and assure that ITC or the employee has a valid license for each program.

d. Maintain a record of authorized and licensed software on each computer and update this record when authorized software is added or deleted.

e. Periodically check the software installed on a sample of computers against the most current record of authorized and licensed software for the computer.

f. Take necessary actions to purchase additional licenses or delete unlicensed software from computers to assure compliance with copyright restrictions.

Commission Response. OIS stated that it would be extremely expensive to track and inventory software on all PCs in the agency and that this is not warranted by any evidence found during the audit or other pattern of abuse in the agency. Agency policy makes each individual responsible for complying with licensing requirements of software installed on his or her computer. OIS also stated that it has purchased and is waiting for resources to install a software metering program for LAN-based software that does not already have a built-in metering system.

Auditors' Additional Comments. ITC's existing policy is not adequate to determine and ensure compliance with licensing requirements for software not on the LAN. The use of "auditing" software enables a person to determine all software installed on a computer. However, unless OIS has an inventory of all software installed on the computers and all licenses, it cannot determine and ensure compliance with licensing requirements.

7. Procedures for Transporting Backup Tapes Are Not Documented

ITC has a contract with a commercial vendor to store its LAN backup tapes at an offsite location. The contractor transports the tapes from ITC to its storage facility in Herndon, Virginia. ITC does not have documented procedures for the contractor or OIS personnel regarding the transporting and releasing of backup tapes to assure the tapes are secure and are not accessible by unauthorized persons. Security and control procedures should be documented to assure that they are known by all parties and tested periodically to assure they are followed.

Based on discussions with the storage contractor, it appears that procedures are in place to safely transport backup tapes between locations. As discussed above, however, OIS should develop and document procedures to assure that the contractor only releases backup tapes to representatives authorized by OIS.

GAO *Standards for Internal Controls in the Federal Government*, Specific Standard No. 1, Documentation, states that internal control systems are to be clearly documented and the documentation is to be readily available for examination.

***Recommendation*.** We recommend that the Director of OIS document the procedures for transporting backup tapes between ITC and the off-site storage facility and procedures for releasing backup tapes to ensure that the tapes are safeguarded from unauthorized use or disposition.

***Commission Response*.** OIS stated that it has requested the contractor to provide brief documentation of its standard procedures for handling backup tapes.

***Auditors' Additional Comments*.** While it is adequate to have the contractor document its standard procedures for handling backup tapes, we think OIS should, at a minimum, review the procedures for consistency with its intended policy and supplement them with a list of persons authorized to handle backup tapes, and their authorization levels.

8. Disaster Recovery Plan Is Not Tested

ITC issued a disaster recovery plan in March 1993, but has not updated or tested this plan. The plan contains contact names of persons who are no longer ITC employees. In addition, ITC has not tested the plan to ensure that:

- Points of contact and their telephone numbers are current and accurate.
- Contact persons are informed about their role and would be readily available in the event of an emergency.
- Hardware and software replacements would be available as required.
- Information about external services is current and accurate.

In testing the disaster recovery plan, ITC should simulate a disaster and perform the necessary steps to recover, such as preparing a list of parts or equipment needing replacement, contacting vendors for availability, recalling backup tapes, and providing interim solutions to LAN users.

OMB Circular A-130, Appendix III, Section 3.c.(3), Disaster and Continuity Plan, states that agencies are to maintain disaster recovery and continuity of operations plans that are fully documented and operationally tested periodically at a frequency commensurate with the risk and magnitude of loss or harm.

***Recommendation*.** We recommend that the Director of OIS update and test its disaster recovery plan and establish procedures to periodically update and test the plan in the future.

Commission Response. OIS stated that the disaster recovery plan has already been updated as recommended and that it will run a simulation to test the plan. The simulation, however, will be limited to checking the validity of phone numbers, etc., due to resource constraints and to avoid disruption of agency work.

9. Titles and Roles of Network Administrators Should Be Clarified

We noted that various ITC directives and publications used different terms to describe network administrators who have access rights to a limited area. For instance, Administrative Announcement FY 91-40 uses the term Local LAN Administrator, Administrative Announcement FY 91-19 uses Local LAN Rep, and ITC Directive 1360.1 uses Designated Systems Administrators or Coordinators. During our review, it appeared that there was not a clear distinction between persons identified as LAN administrators, who have certain access rights, and LAN representatives who have only user access rights and do not operate in the capacity of a network administrator. This caused confusion for office supervisors and users because it was not clear who they should contact about LAN matters or problems.

ITC prepared a Network Administration Standards and Procedures Guide in June 1989, which included tasks and functions that helped the LAN administrators to manage everyday functioning of the LAN and its users. It set standards for performing specific LAN routines and identified procedures to perform LAN tasks correctly and meet established standards. An OIS representative indicated that this document is no longer used and was possibly replaced by the USITC Banyan Network Users' Manual. The users' manual was produced in August 1993, for the purpose of providing a source for end users to better utilize the network resources. It does not include standards and guidelines for network administrators.

GAO *Standards for Internal Controls in the Federal Government*, Specific Standard No. 1, Documentation, states that internal control systems should be clearly documented and the documentation should be readily available for examination.

Recommendations. We recommend that the Director of OIS:

a. Issue a statement to all LAN users clarifying the titles, and describing the roles and responsibilities assigned to each level of LAN administrator.

b. Reissue a Network Administration Standards and Procedures Guide to all LAN administrators.

Commission Response. OIS stated that it does not agree that inconsistency in the use of terms for Network Administrators in various directives results in confusion or impediment to obtaining services or assistance. It stated that it will review and revise the terms for consistency as the documents are modified.

Auditors' Additional Comments. During our review, we noted confusion between the terms and think that a statement identifying duties and responsibilities will be helpful. In addition, we continue to believe that OIS should reissue a Network Administration Standards and Procedures Guide to all LAN administrators.

10. Policies Regarding Non-essential Software and Unofficial Computer Use Should Be Established

We determined that ITC does not have policies or guidance regarding the use of computer equipment for non-official business or the availability of software that is not essential for an employee to perform his or her duties. We could not determine the extent, if any, that employees used computers for non-official business. We did observe, however, that there were two games on the network (in Windows Software) and one game on the C:/ drive of one other computer.

We did not find any specific Federal guidance prohibiting non-essential software on Government computers or the use of Government computers for non-official business. However, the proposed revision to OMB Circular A-130, Appendix III, (Federal Register, Volume 60, No. 63, dated April 3, 1995) stresses management controls such as individual responsibility and accountability rather than technical controls. For instance, an important new requirement for security plans is the establishment of rules of behavior for individual users. These rules should clearly delineate responsibilities and expectations of individuals with access to the system. The rules should cover such matters as unofficial use of government equipment and the assignment and limitation of system privileges. The proposed revision introduces the concept of "least privilege" which restricts the user's access or type of access to the minimum necessary to perform his or her job.

Recommendation. We recommend that the Director of OIS write proposed policies for commissioner approval regarding the use of Government equipment for non-official business and the availability of non-essential software in accordance with the principles of "least privilege."

Commission Response. OIS stated that it does not agree that ITC does not have policies or guidance regarding the use of computer equipment for nonofficial business because it is covered in the mandatory annual Federal employee ethics training by the General Counsel. In addition, guidance on the use of agency facilities to access the Internet and for job-search purposes has been recently issued by the Chairman. OIS does not regard the use of legal but non-essential software as a problem.

OIS stated that with respect to its policy approach to controlling access to information on its computer systems, ITC is in a relatively low-threat environment. Access controls are applied on a need-to-know basis for systems and databases needing protection. For the general LAN systems, OIS believes that maximum sharing of information results in improved work processes and forming of teams across organizational boundaries.

OIS stated that it will review with the General Counsel and make a recommendation on the need and format for guidance on authorized non-official uses of agency computer facilities. It will be along the lines of the GSA guidance on authorized non-official telephone use and existing agency guidance on authorized non-official use of the Internet.

Appendix

UNITED STATES INTERNATIONAL TRADE COMMISSION

WASHINGTON, DC 20436

December 15, 1995

Memorandum **OIS-S-192**

To: The Inspector General

From: Director, Information Services

Subject: Agency response to draft LAN Operations audit report

The subject audit concentrated mainly on security of LAN operations. The results of the review confirm that the agency is maintaining an appropriate balance between cost, user convenience and security in our network operations.

The primary goals of our LAN security policies are to avoid economic loss of staff work product; to avoid compromise of sensitive data; and to discourage employee abuse of software licenses. These goals are based on our assessment of the actual risks in our computing environment, taking into account the level of sensitivity of our data and the likely constraints on parties with a motive for getting unauthorized access to or destroying data on our systems.

The audit found no definite or probable instances of security violations, no evidence of significant loss or destruction of data or other work product, and no evidence of widespread or intentional violations of intellectual property (i.e., illegal software use.)

The specific security weaknesses identified in the report are mainly cases where there is a lack of documentation or a lack of positive control over relatively minor risk factors. However, the auditors did make several worthwhile recommendations that we are implementing or will implement as resources permit.

Our response to the specific findings is as follows. The Office of Information Services (OIS) will complete the actions noted on all issues on or before July 1, 1996.

1. "Security control weaknesses exist regarding use of modems." The auditors recommend implementing much more restrictive controls on modem use in the agency, and new reports on dial-in access traffic. OIS believes the threat from this source is minimal and the cost and inconvenience of the additional reports and restrictions are not justified.

Action item: We will implement closer monitoring of failed attempts to log in to the network via the non-dial-back facility since we have identified a way of doing this that does not involve extensive administrator time.

2. "Unauthorized and fictitious users are not deleted from the network on a timely basis." The "fictitious users" referred to are accounts established for such purposes as network administration, weekend data backup, students using the ITC training room, etc. OIS has a procedure in place that double-checks that program-office LAN administrators have deleted departing employees from the network. The procedure is not perfect and it does involve a delay of up to 1 month from the time the user stops using the network. However, we believe the threat from departing employees is small, and we have never become aware of an actual or suspected case of compromise or destruction of data from this source. The auditors did discover one case where an administrator account was not deleted or deactivated within a few weeks of the departure of an OIS employee, but we were able to positively confirm that his account was never used after the employee's departure, and the data access available to that account was noncritical.

Action item: We will implement an annual review of fictitious accounts to establish the continuing need for each or to delete them.

3. "Procedures for investigating security violations should be strengthened." We believe that the small additional security provided by the measures suggested by the auditors would be very greatly outweighed by the additional time and cost needed to "investigate and resolve all possible security violations" (including the very common occurrence of a failed login attempt.)

Action item: We will re-establish the procedure of recording the network hardware ("token ring") location of unsuccessful logins.

4. "Security Plan should be developed and security controls tested."

Action item: We will develop a security plan that conforms to the draft revised

OMB guidance in Circular A-130.

5. "Unauthorized persons have access to backup tapes." Several OIS staff members other than the network administrators have access to the main computer room as a requirement for performance of their duties. They are thus not "unauthorized," and are subject to the same legal and policy sanctions as administrators for any possible abuse of their access to ITC computer systems. However, we do agree that security could be enhanced somewhat at little or no cost by maintaining a lockbox in the computer room for the storage of backup tapes.

Action item: We will implement a tape lockbox in the computer room.

6. "Procedures for assuring compliance with software licensing requirements are inadequate." It would be extremely expensive for the agency to attempt to track and inventory software on all PCS in the agency. Nor is this warranted by evidence from the audit or otherwise of any pattern of abuse in the agency. Agency policy clearly makes each employee responsible for complying with licensing requirements of software they may install or permit to be installed on their computers. A reminder of this policy was sent to all employees this past summer, along with an offer to make "auditing" software from the Software Products Association available to individuals or managers who want their PCs or those in their units checked. Licenses for LAN-based software are clear enough in most cases that no special tracking procedure is needed. For example, we have agencywide licenses for e-mail and wordprocessing software. To help us track usage for license-compliance purposes where that is necessary because the vendor does not provide built-in metering we have bought and are waiting for resources to be available to install a software metering program.

Action item: We will implement software metering for LAN-based software as needed and feasible.

7. "Procedures for transporting backup tapes are not documented."

Action Item: We have asked the contractor to provide brief documentation of their standard procedures for handling tapes.

8. "Disaster recovery plan is not tested."

Action item: The ITC Disaster Recovery Plan has already been updated as recommended. We will run a simulation to test the plan. (However, we will limit the simulation to checking the validity of phone numbers, etc. in view of resource constraints and to avoid disruption of agency work.)

9. "Titles and roles of network administrators should be clarified." We do not agree that inconsistency in use of the terms "Local LAN Administrator" and "Local LAN Representative" in various directives results in significant confusion (of agency staff) or impediment to obtaining services or assistance.

Action item: We will review the use of the terms "LAN administrator" and "LAN Representative" in agency guidance publications and revise them for consistency as the documents are modified.

10. "Policies regarding non-essential computer use should be established." We disagree that "the ITC does not have policies or guidance regarding the use of computer equipment for nonofficial business. . ." This is very adequately covered in the mandatory annual Federal employee ethics training given to every employee by the General Counsel. Guidance on specific issues related to use of agency facilities for accessing the Internet have been issued recently, and guidance and specific authorization to use agency computer facilities for job-search purposes during the RIF period has also been issued by the Chairman.

We do not regard use of legal but "non-essential" software as a problem. Such products might include screen savers, personal information managers (like a Rolodex, but electronic) and other "personal productivity" software that may be in the public domain or may be owned by employees.

With respect to our policy approach to controlling access to information on our computer systems, we start from the fact that we are in a relatively low-threat environment, so that measures designed for defense, intelligence or financial systems are inappropriate. Where we do have systems or databases that need protection, like confidential Dockets submissions, we apply access controls on a need-to-know basis. However, for our general LAN systems we believe that maximum sharing of information encourages the creative and entrepreneurial efforts of staff to use all available tools to improve their work processes and form teams across organizational boundaries.

Action item: OIS will review with the General Counsel and make a recommendation on the need for and appropriate format for guidance on authorized non-official uses of agency computer facilities, along the lines of the GSA guidance on authorized non-official telephone use and the existing agency guidance on authorized non-official uses of the Internet.

Chairman's approval of agency response to draft audit report

Pete Watson

Chairman Peter S. Watson

Date: 1-18-96