Office of
INSPECTOR GENERAL

Audit Report

Review of USITC's Local Area Network
Administration and Controls

Report No. IG-04-92

September 1992

Date Issued

INSPECTOR GENERAL

UNITED STATES INTERNATIONAL TRADE COMMISSION

WASHINGTON, D.C. 20436

September 17, 1992

REVIEW OF USITC'S LOCAL AREA NETWORK ADMINISTRATION AND CONTROLS

During the last few years, the Commission has invested a substantial amount of money and effort into automating agency functions and specifically in implementing the Local Area Network (LAN). The overall objective of this review was to determine whether the Commission has implemented a program that ensures effective management and operation of the LAN system.

This review was conducted by Cotton & Company in accordance with the Government Auditing Standards issued by the Comptroller General of the United States. The results of their review are presented as an attachment to this report. They found that the Commission's procedures were sufficient, in all material respects, to provide for effective LAN administration and control.

The auditors had the following findings:

-- Dial-up telephone access to the LAN is not properly secured;

-- The LAN files for two offices are not backed up on weekends;

-- A policy does not exist establishing a frequency standard for virus checking and the practice throughout the Commission is inconsistent;

-- A formal system or procedures does not exist to identify the type and number of software packages purchased or in use which is needed to demonstrate compliance with Federal licensing statutes;

-- A policy statement does not exist concerning the unauthorized use or duplication of copyrighted software;

-- A disaster recovery or contingency plan does not exist for offsite operation of the LAN in the event of a catastrophic incident; and

-- The LAN administrator's internal control responsibilities are not set forth in a formal statement.

Three matters were noted for management's consideration. 1) Electronic access keys issued to employees are not routinely deactivated upon termination of employment. 2) The LAN user manual does not contain current and complete user information. 3) Commission employees not in the Office of Administration reported a deterioration in the quality of LAN support, which we attribute at least in part to the extended vacancy of the Chief position in the Office Automation and Support Division.

Recommendations relating to the findings are presented on pages 6 through 8 of the report. In summary, we recommend that the Director of Administration implement appropriate policies and procedures or take other needed actions concerning call-back controls, weekend backups, virus scans, software inventory, unauthorized copying of software, disaster recovery (contingency) plans, and LAN internal controls.

The Director of Administration generally agreed with the findings and recommendations. A summary of the Director's comments on the findings and our responses are presented on page 8 of the report. The Director's comments are presented in their entirety as an appendix to the report.

Jane E. Altenhofen

Jane E. Altenhofen
Inspector General

Attachment

TABLE OF CONTENTS

Attachment	-	Report on the Review of the USITC's Local Area Network Administration and Controls
Appendix	-	Memorandum from Director, Office of Administration, dated August 12, 1992, on Draft Report

Attachment

REPORT ON THE REVIEW OF THE UNITED STATES INTERNATIONAL TRADE COMMISSION'S LOCAL AREA NETWORK ADMINISTRATION AND CONTROLS

Prepared by:

Cotton & Company
Certified Public Accountants
Alexandria, Virginia

COTTON & COMPANY

CERTIFIED PUBLIC ACCOUNTANTS

100 SOUTH ROYAL STREET • ALEXANDRIA, VIRGINIA 22314 • (703) 836-6701 • TELECOPIER: (703) 836-0941

DAVID L. COTTON, CPA
CHARLES HAYWARD, CPA
BRENDA N. BURZENSKI, CPA
MICHAEL W. GILLESPIE, CPA
ROBERT L. FLESHER, CPA
KEVIN P. MCFADDEN, CPA
CATHERINE L. NOCERA, CPA
ELLEN P. REED, CPA

June 4, 1992

Ms. Jane E. Altenhofen
Inspector General
United States International Trade Commission
500 E Street, SW
Washington, DC 20436

Dear Ms. Altenhofen:

We reviewed the United States International Trade Commission's (ITC) policies and procedures for managing its Local Area Network (LAN). Our overall objective was to determine if ITC has implemented a program that ensures effective management and operation of the LAN system. Specific objectives were to determine if ITC:

- Administrative Management: Effectively performs the basic management functions of planning, organizing, directing, and controlling LAN resources.

- Configuration Management: Maintains adequate documentation concerning the components and configuration of its LAN, implements and enforces standards for network components and configurations, and adequately controls changes to network components and configurations.

- Managing Network Availability and Performance: Establishes effective methods and procedures to ensure that network resources are available to users to the maximum extent needed and that network resources perform with needed speed, efficiency, and accuracy.

- Application Management: Maintains adequate documentation on its application software, implements standards and enforces licensing and copyright restrictions for software, and controls changes to its applications software.

- User Support: Provides effective user support through training, ongoing technical support, and an information exchange program.

- Cost: Maintains a control system that monitors LAN costs and determines the actual costs incurred to acquire, install, and operate the LAN.

- Security: Provides effective security over LAN information resources through a formal ADP security program incorporating written policies and procedures that meet Federal laws and regulations.

We performed our review in accordance with generally accepted Government auditing standards. Our review included the tests and procedures we deemed necessary to meet the review objectives described above.

Our review was made for the limited purpose described above and, as such, would not disclose all material weaknesses in ITC's internal control system. Accordingly, we do not express an opinion on ITC's internal control system taken as a whole.

Based on our review for the limited purposes described above, ITC's procedures were sufficient, in all material respects, to provide for effective LAN administration and control. Our review did, however, disclose several conditions that we believe warrant corrective action. In addition, we noted certain other matters for management's consideration. The review results are described in detail in the accompanying report.

We discussed our review results with the Director, Office of Information Resource Management (OIRM); the acting chief of Office Automation Support Division; the senior network administrator; the special assistant for OIRM planning; and other headquarters personnel responsible for the overall management of ITC's LAN.

The accompanying report is intended solely for ITC's information and use and should be used for no other purpose.

Very truly yours,

COTTON & COMPANY

By: Kevin P. McFadden

Kevin P. McFadden, CPA

CONTENTS

Part		Page
1	INTRODUCTION	1
	Background	1
	Objective	2
	Scope	2
	Methodology	2
2	REVIEW RESULTS	4
	Findings	4
	Other Matters for Consideration	6
	Recommendations Regarding Findings	6
	Suggestions Regarding Other Matters for Consideration	8
	APPENDIX	
	Commission's Response	

REPORT ON THE REVIEW OF THE UNITED STATES INTERNATIONAL TRADE COMMISSION'S LOCAL AREA NETWORK ADMINISTRATION AND CONTROLS

PART 1. INTRODUCTION

In this part, we discuss the review background, objective, scope, and methodology.

BACKGROUND

The United States International Trade Commission (ITC) is an independent Federal agency with six commissioners, a staff of about 500, and Fiscal Years (FY) 1991 and 1992 budgets of $40,299,000 and $42,434,000, respectively.

During the past few years, ITC has invested a substantial amount of money and effort into automating agency functions. Virtually every employee has a personal computer linked to the Local Area Network (LAN) system, which became operational in 1988.[1] The primary LAN system is Banyan Vines. The Office of Tariff Affairs and Trade Agreements (TATA) is currently connected to two LAN systems, the Banyan Vines and Novell; the latter is in the process of being phased out. In December 1991, ITC issued *A Five-Year Plan for Information Resources Management* that outlines major changes planned for the LAN.

As of January 1992, the general-purpose LAN consisted of 11 Banyan file servers and approximately 470 personal computers as workstations. The system includes two modem pools offering dial-out service to other facilities. A limited dial-in service is also provided.

The LAN supports a variety of office automation functions including word processing, electronic mail, spreadsheets, and end-user data-base applications. The system contains unclassified and sensitive information, such as confidential (proprietary) business information. Applications software includes WordPerfect, Lotus Networker, dBase III, and Harvard Graphics. Users are given LAN training and a guide prior to using the system.

As set forth in USITC Directive 1028.1, dated April 21, 1991, the Office of Information Resources Management (OIRM) is responsible for coordinating and maintaining ITC's data collection, statistical support, public reporting, and information processing activities. Within OIRM, the Office Automation Support Division is responsible for all network administration and office automation technical support. The network administration includes all LAN connectivity and communications interfaces with computer service bureaus and mainframes, network hardware, software, maintenance, cabling, user support, and standards.

---

[1]A LAN is a geographically confined computer-based communication system capable of transmitting information or data between stations.

Technical support includes the installation, maintenance, and support for a wide range of end-user software and providing end-users with supplies and services as needed.

OBJECTIVE

The overall objective of this review was to determine if ITC has implemented a program that ensures effective management and operation of the LAN system. The objective encompasses the following elements:

- Administrative management
- Configuration management
- Managing network availability and performance
- Application management
- User support
- Cost
- Security

SCOPE

We conducted our review at ITC headquarters in Washington, DC, from May 5 to June 4, 1992.

We conducted numerous discussions with the senior network administrator and the special assistant for OIRM planning. We also met with other ITC personnel responsible for the overall management of ITC's LAN, including representatives from the Offices of Industries, Investigations, Economics, and TATA.

METHODOLOGY

We gathered data for our review through interviews and analyses of policies, documents, and reports determined to be important to the process of managing ITC's LAN.

The major guidelines and operating regulations we used to evaluate the management and administration of ITC's LAN included the following criteria:

- Office of Management and Budget (OMB) Circular A-11, *Preparation and Submission of Budget Estimates*, Section 43: Data on Acquisition, Operation, and Use of Information Technology Systems.

- OMB Circular A-130, *Management of Federal Information Resources*.

- General Services Administration's (GSA) *Federal Information Resources Management Regulation* (FIRMR), Part 201-7, Security of Information Resource Systems.

- GSA's FIRMR Part 201-19, Section III, *IRM Review Handbook*, "Management of IRM Activities."

- 5 *Code of Federal Regulations*, Subpart C, Section 930.301, Training Requirement.

- U.S. Department of Commerce National Bureau of Standards' *Federal Information Processing Standards* Publication No. 112, "Password Usage."

- Computer Security Act of 1987 (Public Law 100-235, Section 5).

- Office of Personnel Management's *Federal Personnel Manual*, Chapter 732, "Personnel Security."

- 18 USCS §1030, pages 291-293, "Fraud and False Statements."

- Robert R. Moeller's *Computer Audit, Control, and Security*; Wiley, 1989; Chapter 4, "Controls in the Distributed Network," and Chapter 11, "Auditing End User Computing General Controls."

- ITC Guidelines:

  - Directive 1028.1, Office of Information Resources Management Mission and Function Statement, dated April 21, 1991.

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

  - Directive 1360, Automated Data Security Procedures, dated June 27, 1988.

  - Administrative Notice ITC-N-6001, Eating, Drinking, and Smoking While Operating ADP and Wang Equipment, dated November 28, 1986.

  - Administrative Announcement USITC FY-91-40, Issuance of Identification Badges and Access to the Local Area Network, dated May 15, 1991.

The review was conducted in accordance with the Comptroller General's *Government Auditing Standards* (1988 revision).

REPORT ON THE REVIEW OF THE UNITED STATES INTERNATIONAL TRADE COMMISSION'S LOCAL AREA NETWORK ADMINISTRATION AND CONTROLS

PART 2: REVIEW RESULTS

Our findings, other matters for consideration, conclusions, and recommendations are discussed in this part.

FINDINGS

We noted certain conditions related to the management and administration of ITC's LAN that warrant management's attention. These conditions are discussed below:

1. Dial-in telephone access into the LAN is not properly secured. When a processing system provides "dial-in" access, industry standards stipulate that certain control features be used, including a dial-back system or similar modem restriction. ITC Directive 1360, Chapter B, Section 6, requires that dial-in access to stand-alone microcomputers containing CBI (Confidential Business Information) "contain additional security/ communications software which prompts the user for a sign-on password and activates a dial back feature." The LAN contains CBI.

   At present, the potential exists for compromise of LAN security. We documented one case where an individual has dial-in access to the LAN via a modem on the workstation without the dial-back feature being activated. This same individual has complete access to <u>all</u> records, documents, and data stored on a file server.

   An unknown number of additional LAN users currently maintain dial-in access. LAN administrators do not know if they are using the dial-back feature. Further, it is possible for an individual user with a dial-in modem to completely bypass LAN security without LAN administrators being aware of it.

   Prior to our review, OIRM recognized this problem and proposed a solution. We have incorporated certain aspects of its proposal into our recommendation.

2. Because of the amount of work done on weekends, ITC has identified a need for a weekend back-up service. All file servers on the LAN have their weekend files backed up except for the Offices of Industries and Investigations. These offices have specifically requested weekend backup service; they have, however, denied OIRM access to the file servers because of the sensitive nature of the files. Without this access, OIRM cannot provide the needed weekend backup service. ITC Directive 1028.1 makes OIRM responsible for providing this service.

3. ITC does not have a policy describing a frequency standard for virus checking. Without a standard, no procedure exists to determine if the file servers' scanning frequency is adequate. The file servers supported by OIRM are scanned 5 days a week, the Office of Investigations scans twice a week, and the Office of Industries every 3 days. Without access to all file servers (as discussed in Finding No. 2), OIRM cannot provide standardized virus checking. ITC Directive 1028.1 makes OIRM responsible for providing this service.

4. ITC has no formal system or procedures to identify the type and number of software packages purchased or in use. Purchased software is not tracked in the personal property (or other control) system. As such, it cannot demonstrate compliance with Federal licensing statutes. A related negative effect of this condition is that ITC could lose available discounts when software upgrades are purchased, if it is unable to identify and document the number of original units purchased.

5. No formal ITC statement of policy exists concerning the unauthorized use or duplication of copyrighted software by ITC employees. The US Code, Chapter 5, Copyright Infringement and Remedies, Title 17, Copyrights, states: "Anyone who violates any of the exclusive rights of the copyright owner...is an infringer of the copyright." Computer software by its nature is easily duplicated. ITC has considered the need for such a directive, but the responsible parties have been unable to agree on the directive's content and wording. Without such a directive, ITC may become responsible if employees violate the copyright law.

6. ITC has no disaster recovery or contingency plan for offsite operation of the LAN in the event of a catastrophic incident. ITC has identified the need for a disaster recovery or contingency plan in its 5-year plan, *A Five-Year Plan for Information Resources Management*. Although the 5-year plan identified a June 30, 1992, milestone for a plans and procedures handbook for disaster recovery/contingency operation, ITC management indicated that planning is in the "early developmental stages." Without its LAN capability, ITC would have difficulty carrying out its statutory responsibilities.

7. ITC has no formal statement of the LAN administrator's internal control responsibilities. Presently, ITC's primary LAN system (Banyan Vines) produces various summaries of user and system status and activity. The senior network administrator periodically reviews the on-line logs to ensure that certain administrative tasks have been accomplished; however, this is only done when time permits. ITC should have a formal internal control plan for its LAN that includes procedures designed to prevent, at a minimum, destruction of data, data security degradation, and unauthorized access to CBI.

OTHER MATTERS FOR CONSIDERATION

We noted certain other matters that the Director of Administration, should consider for action. These follow:

1. Electronic access keys issued to employees are not routinely deactivated upon termination of employment. ITC has no policy to routinely deactivate the electronic keys at the time of employee termination. FIRMR Part 201-7.105(d)(1) requires that authorized personnel be positively identified through the use of local access control procedures. As part of our review, we identified former employees on the access list to the computer room.

2. The *USITC LAN Training* user manual does not contain current and complete user information. As such, LAN users do not have access to sufficient, current documentation concerning ITC's policies and procedures regarding its LAN operations. As a result, users may be unaware of policies and procedures regarding LAN use, it may take more time for them to become proficient in using the LAN, and they may never learn to use some of its features.

3. During our interviews of selected LAN file servers and users, certain respondents reported a deterioration in the quality of LAN support services. Because of a hiring freeze, the position of Chief, Office Automation Support Division, is vacant. OIRM staff have attempted to perform the necessary duties in the interim.

RECOMMENDATIONS REGARDING FINDINGS

Our recommendations to strengthen policies and procedures related to the Findings section are presented below. These recommendations are in the same order in which the findings were presented.

1. The Director of Administration should instruct the Director, OIRM, that all dial-in modems should use the dial-back control feature. Directive 1360 should be revised, updated, and clarified.

   Modem restrictions should be employed for incoming calls to the LAN. Specifically, dial-in access to the LAN should be permitted only through a bank of personal computers set up in the computer room that run software that requires: (1) a password for connection, (2) activation of a dial-back facility, and (3) automatic capture of user identification for anyone using the facility. Activity should be logged and monitored on this bank of personal computers, and questionable log entries should be investigated.

2. The Director of Administration, working with the Director of Operations, should make arrangements for OIRM to be granted, at a minimum, "read-only" access to perform weekend backups in accordance with its responsibility under ITC Directive 1028.1.

3. The Director of Administration, working with the Director of Operations, should make arrangements for OIRM to be granted, at a minimum, read-only access to perform virus scans in accordance with its responsibility under ITC Directive 1028.1.

4. The Director of Administration should instruct the Director, OIRM, to complete an inventory of each software package purchased and the number of copies currently in use. ITC is planning to upgrade the entire LAN over the next 12 to 18 months. As part of the upgrade, ITC plans to acquire upgraded versions of much of the software currently in use. To obtain the upgrade price for the new software, ITC must be able to document how many copies of each package have been purchased.

   ITC should consider developing a formal system for identifying, counting, and controlling the number of copies of software on the LAN. The system should be capable of documenting compliance with Federal licensing standards and readily identifying the type and number of software packages purchased.

5. The Director of Administration should issue a directive prohibiting the unauthorized copying of copyrighted software. The directive might consist of nothing more than a statement to the effect that "ITC adheres to the tenants of United States Code, Title 17, which expressly prohibits unauthorized duplication of copyrighted materials."

6. The Director of Administration should assess the status of the disaster recovery (contingency) plan's development and take action to see that the project is completed expeditiously.

7. The Director of Administration should instruct the Director, OIRM, to standardize and document procedures for the routine checking of LAN-produced lists and summaries. This should include the procedures currently conducted informally by the senior network administrator and OIRM staff to ensure effective internal control as well as any additional tasks OIRM considers necessary.

   The following additional checks should be considered for inclusion:

   - A periodic check of logs to identify unusual cases of unauthorized access attempts.

   - A periodic check of LAN account "last access" dates to identify and explain accounts left idle for long periods of time.

   - A periodic check of account access privileges to ensure that no individual is allowed inappropriate access rights.

   At a minimum, the procedures should specify an internal control objective and plan for the LAN, the minimum frequency of completion of the control tasks, and the individual who is responsible for each task. Performance

standards should be altered to reflect these new responsibilities. Third-party software may be available to automate many of these routine, repetitive processes.

Commission Comments

The Director of Administration responded in writing to our recommendations (see appendix). He agreed with our recommendations and provided comments on the actions taken and those that are planned. These actions should result in improved administration and control over ITC's LAN.

SUGGESTIONS REGARDING OTHER MATTERS FOR CONSIDERATION

Our suggestions regarding other matters for consideration are presented below.

1. The Director of Administration should instruct the Director, Office of Management Services, to implement a policy of deactivating electronic access keys upon termination of employment. All keys belonging to former employees should be assembled and deactivated.

2. The Director of Administration should instruct the Director, OIRM, to upgrade the *USITC LAN Training* to include, at a minimum, the topics listed under the caption, "Network Training." The manual should also include copies of policies or directives that users might require.

Commission Comments

The Director of Administration responded in writing to our suggestions regarding other matters for consideration (see appendix). He agreed with our suggestions and provided comments on the actions taken and those that are planned. These actions should result in improvements regarding the administration and control over ITC's LAN.

Appendix

AD-P-528

UNITED STATES INTERNATIONAL TRADE COMMISSION

August 12, 1992

MEMORANDUM

TO: Inspector General

FROM: Director, Office of Administration

SUBJECT: Draft Report, "Review of USITC's Local Area Network Administration and Controls"

As requested by your memorandum dated July 16, 1992 (IG-P-038), submitted herewith is the Office of Administration's response to the subject draft audit report issued July 16, 1992. In accordance with Section 11 of the USITC Directive 1701, the Commissioners have had an opportunity to comment on the response and the Chairman has approved it with modifications.

The Office of Administration agrees with all the audit recommendations. The attached response includes the actions to be taken and the target completion dates.

Please call me at 205-3131 or Bill Stuchbery at 205-3135 if you have any questions.

ATTACHMENTS

cc: Director, Office of Information Resources Management
Director, Office of Management Services

ADMINISTRATION'S COMMENTS ON THE DRAFT REPORT

RECOMMENDATIONS REGARDING FINDINGS

RECOMMENDATION:

1. The Director of Administration should instruct the Director, OIRM that all dial-in modems should use the call-back control feature. Directive 1360 should be revised, updated, and clarified.

   Modem restrictions should be employed for incoming calls to the LAN. Specifically, dial-in access should be permitted only through a bank of personal computers set up in the computer room that run software that requires: (1) a password for connection, (2) activation of a dial-back facility, and (3) automatic capture of user identification for anyone using the facility. Activity should be logged and monitored on this bank of personal computers, and questionable log entries should be investigated.

RESPONSE: AGREE

Revision of Directive 1360 was started as part of the Administration's directives update procedure and prior to the IG conducting a study on LAN Administration and Controls. There is a chronology of events associated with the completion of the revision of Directive 1360 in that it cannot be completed until other recommendations are implemented and procedures written to be incorporated in the Directive. Therefore the revision to Directive 1360 is scheduled to be completed 30 days after the completion of the "dial-in/call back" system as identified below.

TARGET COMPLETION DATE: January 29, 1993

Working with the Information Security Committee, OIRM will institute a central network dial-in facility with call-back, password, and capture of user ID to be installed in the ITC Computer Room. Logs of use will be periodically reviewed. All Commission-owned copies of "Carbon-Copy", "Pc-AnyWhere", and any other software which allows dial-in access to individual PCs with modems will be collected by OIRM. This procedure will be incorporated into Directive 1360 and will state that users are not allowed to dial-into their individual PCs.

A target completion date of 12/31/92 has been chosen since software must be purchased and PCs which will be turned in as a result of the ORS II purchase (approved August 3, 1992) will be used for the central network dial-in facility. Once the "dial-in/call back" system has been fully tested and implemented, the procedures will be incorporated into Directive 1360.

TARGET COMPLETION DATE: December 31, 1992

RECOMMENDATION:

2. The Director of Administration, working with the Director of Operations, should make arrangements for OIRM to be granted, at a minimum, "read-only" access to perform weekend backups in accordance with its responsibility under ITC Directive 1028.1

RESPONSE: AGREE

The Directors of Administration and Operations should work out an agreement whereby the Director of Operations will instruct the Directors of Industries and Investigations to place OIRM's Senior Network Administrators on their Server Adminlists. (OIRM will then take immediate action to include those offices in the already established week-end back-up procedures.)

TARGET COMPLETION DATE: October 30, 1992

RECOMMENDATION:

3. The Director of Administration, working with the Director of Operations, should make arrangements for OIRM to be granted, at a minimum, "read-only" access to perform virus scans in accordance with its responsibility under ITC Directive 1028.1

RESPONSE: AGREE

The Director of Operations should instruct the Directors of Industries and Investigations to place OIRM's Senior Network Administrators on their Server Adminlists. (OIRM will take immediate action to include those offices in OIRM's established virus scanning procedures.)

TARGET COMPLETION DATE: October 30, 1992

RECOMMENDATION:

4. The Director of administration should instruct the Director, OIRM, to complete an inventory of each software package purchased and the number of copies currently in use. ITC is planning to upgrade the entire LAN over the next 12 to 18 months. As part of the upgrade, ITC plans to acquire upgraded versions of much of the software currently in use. To obtain the upgrade price for the new software, ITC must be able to document how many copies of each package have been purchased.

ITC should consider developing a formal system for identifying, counting, and controlling the number of copies on the LAN. The system should be capable of documenting compliance with Federal licensing standards and readily identifying the type and number of software packages purchased.

RESPONSE: AGREE (with Qualification)

The OIRM network administrators will develop an inventory system for all purchased software used on the 'network'. This inventory will be updated as new software is purchased and include office/individual initially issued software (if standalone copy) or server loaded on (if LAN copy). OIRM will track the development of third party, Banyan compatible, network tools for software control and consider implementing when an appropriate package is identified.

To the extent possible, OIRM will research and acquire software to scan individual PCs for all software in use, including that software acquired prior to the new inventory being established. Completion of this task for the entire Network will also require the Director of Operations to instruct the Directors of Industries and Investigations to place OIRM's Senior Network Administrators on their Server Adminlists. Without the availability of an appropriate software tool, it would be too time consuming and of questionable value to inventory all software 'in use' on individual PCs just prior to the phaseout of those PCs.

TARGET COMPLETION DATE: March 31, 1993

RECOMMENDATION:

5. The Director of Administration should issue a directive prohibiting the unauthorized copying of copyrighted software. The directive might consist of nothing more than a statement to the effect that "ITC adheres to the tenants of Title 17, U.S.C., which expressly prohibits unauthorized duplication of copyrighted materials."

RESPONSE AGREE

We will forward to the Chairman for approval an Administrative Order prohibiting the unauthorized copying of copyrighted software. This prohibition will subsequently be made a part of ITC Directive 1360.

TARGET COMPLETION DATE: September 15, 1992

RECOMMENDATION:

6. The Director of Administration should issue the status of the disaster recovery (contingency) plan's development and take action to see that the project is completed expeditiously.

RESPONSE: AGREE

This will be part of an overall emergency recovery plan which includes information security, documents protection, facilities protection and relocation as well as the IRM contingency plans. This is included in the Director of Administration's SES work plan. He will give periodic status updates to the Chairman's office.

TARGET COMPLETION DATE: January 15, 1993

RECOMMENDATION:

7. The Director of Administration should instruct the Director, OIRM, to standardize and document procedures for the routine checking of LAN produced lists and summaries. This should include the procedures currently conducted informally by the senior network administrator and OIRM staff to ensure effective internal control as well as any additional tasks OIRM considers necessary.

The following additional checks should be considered for inclusion:

- A periodic check of logs to identify unusual cases of unauthorized access attempts.

- A periodic check of LAN account "last access" dates to identify and explain accounts left idle for long periods of time.

- A periodic check of account access privileges to ensure that no individual is allowed inappropriate access rights.

At a minimum, the procedures should specify an internal control objective and plan for the LAN, the minimum frequency of completion of the control tasks, and the individual who is responsible for each task. Performance standards should be altered to reflect these new responsibilities. Third-party software may be available to automate many of these routine, repetitive processes.

RESPONSE: AGREE

OIRM will document the procedures, standards, and responsibilities for monitoring the network, and include the additional checks recommended by the Auditors. These will be incorporated into a standard Internal Control procedure for

annual follow-up.

A target completion date of May 28, 1993 has been chosen to allow the new Chief, Office Automation Support Division time to become familiar with his or her duties and responsibilities. The Chairman approved on August 3, 1992, a waiver to the Commission's hiring moritorium to fill this position.

TARGET COMPLETION DATE: May 28, 1993

SUGGESTIONS REGARDING OTHER MATTERS FOR CONSIDERATION:

1. The Director of Administration should instruct the Director, Office of Management Services, to implement a policy of deactivating electronic access keys upon termination of employment. All keys belonging to former employees should be deactivated.

RESPONSE: AGREE

Although there were former employees on the access list to the computer room, their access keys were in a safe under the control of the Security Officer in OMS. To maintain the accuracy of the access list the Security Officer is now notifying Kastle Co. to deactivate the keys as they are returned.

TARGET COMPLETION DATE: Completed

2. The Director of Administration should instruct the Director, OIRM, to upgrade the USITC LAN Training Manual to include, at a minimum, the topics listed under the caption, "Network Training." The manual should also include copies of policies or directives that users might require.

RESPONSE: AGREE

The Senior Network Administrator responsible for conducting the Network Training class, will re-write the manual according to the recommendations in the Inspector General's report.

TARGET COMPLETION DATE: February 26, 1993