July 18, 1997

MEMORANDUM

SUBJECT: **Final Report:** Security of Small Purchase Electronic Data Interchange (SPEDI) Local Area Networks (LANs)
Audit Report No. E1AMR7-15-7012-7100307

FROM: Patricia H. Hill, Director
ADP Audits and Assistance Staff (2421)

TO: Paul A. Wohlleben, Director
Office of Information Resources Management (3401)

Betty L. Bailey, Director
Office of Acquisition Management (3801F)

Mark Luttner, Acting Deputy Director
Office of Planning, Analysis, and Accountability (2721)

Attached is our final report entitled "Security of Small Purchase Electronic Data Interchange (SPEDI) Local Area Networks (LANs)." The primary objectives of the audit were to: 1) survey the production SPEDI sites to verify the adequacy of security policy, controls, and documentation for the SPEDI application and the LANs where it is processed; and 2) to verify both physical and logical security controls at the SPEDI Headquarters site. This report represents the opinion of the Office of Inspector General (OIG) and describes problems and recommended corrective actions the OIG has identified.

In accordance with EPA Order 2750, you, as action officials, are required to provide this office a written response to the report within 90 days of the final report date. If corrective actions will not be complete by the response date, we ask that you describe the actions that are ongoing and provide a timetable for completions. In addition, please track all action plans and milestone dates in the Management Audit Tracking System.

We appreciate your many comments to the recommendations presented in the report and the many actions you and your staffs have already initiated to address issues concerning the security of the SPEDI application and its LANs. We have no objection to the further release of this report to the public. Should you or your staff have any questions regarding this report, please contact Jim Rothwell, ADP Team Leader, ADP Audits and Assistance Staff, at (202) 260-1785.

Attachment

Office of Inspector General

Report of Audit

SECURITY OF SMALL PURCHASE ELECTRONIC DATA INTERCHANGE (SPEDI) LOCAL AREA NETWORKS (LANs)

JULY 18, 1997

Audit Report E1AMR7-15-7012-7100307

Inspector General Division Conducting the Audit:	ADP Audits and Assistance Staff
Region(s) Covered:	Regions 1 through 10 Headquarters
Program Offices Involved:	Office of Acquisition Management Office of Planning, Analysis, and Accountability (part of OCFO) Office of Information Resources Management

SPEDI SECURITY CONTROLS NEED IMPROVEMENT

RESULTS IN BRIEF

Survey results revealed that security controls need improvement at all of the responding production SPEDI site. The survey also indicated significant shortcomings in documentation of security controls at both application and Local Area Network (LAN)/facility level, as well as disaster recovery procedures and contingency planning. Five production sites issued no response to our survey by either the LAN System Administrator (SA) or Information Security Officer (ISO) and, therefore, we have no assurance that any of these five sites have proper controls. We consider the absence of management-approved security plans for the SPEDI application and LANs to be a serious control deficiency, because there is a high risk of potential loss or manipulation of critical procurement data. Our survey revealed varied reasons for the inadequate amounts of security documentation and inconsistent implementation of security controls at the production SPEDI sites. For example, Agency-wide security policy and guidance, implementing the most recent OMB Circular A-130, has not been finalized. In addition, personnel were unaware that there is interim EPA guidance to assist in the development of the required security documentation. There is also no coordinated overall security documentation for the SPEDI application production sites. Furthermore, 'assessable unit' managers are confused about OMB Circular A-130 security plan requirements and related requirements identified for OMB Circular A-123.

PURPOSE

As part of the analysis of General Controls for the 1996 Audit of Financial Statements, we evaluated the security controls for the Small Purchases Electronic Data Interchange (SPEDI). At the time of our evaluation, SPEDI was in production at thirteen sites. These sites include the 10 regions, Headquarters and at two Contract Management Division sites [Cincinnati and Research Triangle Park (RTP)]. The focus of this audit was on the development and implementation of security policy and procedures for LANs that process the application SPEDI. We performed a more detailed audit of security implementation at the Headquarters SPEDI site. The detailed audit focused on the presence of logical and physical security controls for that particular site

BACKGROUND

SPEDI is a part of the Integrated Contract Management System (ICMS) which electronically handles small purchases. SPEDI directly obtains information on commitments from the Integrated Financial Management System (IFMS). The procurements or obligations it creates are entered manually into the IFMS system, although this is scheduled to become an electronic interface in the future. In fiscal 1996 SPEDI handled over $44 million in purchases. This figure will increase in future fiscal years as SPEDI is implemented at additional sites and as more vendors use electronic data interchange to conduct business. SPEDI is scheduled to be put into production at EPA laboratories in fiscal 1997.

As the number of production sites grow, the more significant SPEDI's role in EPA's procurement will become. SPEDI is a client/server [1] application which is listed as a 'Major Regional or Program System (Level II)' in EPA's Information System Inventory. This designation reflects the increasing reliance of the Agency on LANs as a means of transmitting key information for conducting Agency business. Although EPA has published LAN Directives and a LAN Operations and Procedures (LOPS) Manual, little audit work has been performed to verify the implementation of security for LANs and LAN-based applications.

SCOPE AND METHODOLOGY

We surveyed thirteen sites where SPEDI was in production as of September 1996. This survey consisted of a set of questions directed to the Information Security Officer (ISO) and to the LAN Systems Administrator(s) (SAs) at each site**.** Questions covered the following subjects: documentation of application and general support system security; implementation of logical and physical security controls; monitoring and reporting security problems; virus protection; training; and any security or performance problems encountered.

The documentation requested in the survey included: 1) an Application Security Plan; 2) a LAN/ Facility Security Plan and 3) a Disaster Recovery/Contingency Plan. Application Security Plans and Disaster Recovery/Contingency Plans were required prior to the OMB Circular A-130 revision in February 1996. The LAN/Facility Security Plan was a new requirement in February 1996.

[1] A decentralized application where locally centralized databases (server) are accessed by individual users via applications on their desktop PCs (client). A Local Area Network (LAN) connecting the PCs and Server provides access capability. These local databases may, in turn, feed into and be refreshed from information maintained in a larger consolidated database.

Furthermore, OMB Circular A-130 stated that the previous requirements remained in effect until NIST issues expanded security planning guidance for the Agency to use for the security plans. We wanted ISOs and LAN Managers to provide security documentation whether the old version or current.

We also performed a detailed evaluation of the Headquarters SPEDI LAN located in the Fairchild Building in Washington, D.C. This evaluation was performed in two phases: 1) a walkthrough to observe implementation of facility security; and 2) an analysis of the operating system (NETWARE) security, as implemented on the SPEDI Headquarters server known as DCFC1. The LAN security monitoring package entitled Omniguard/Enterprise System Manager (ESM), by AXENT Technologies, was used to analyze the NETWARE operating system security. This monitoring software has been tested by the Security Office of the Enterprise Technical Systems Division (ETSD) in Research Triangle Park, North Carolina. The criteria this software uses to evaluate NETWARE Security can be customized and, therefore, was set to reflect EPA Policy and Operational Directives. Additionally, we risk-ranked controls identified by the ESM as "high", "moderate" or "low"[2]. We based these rankings on: 1) scores provided by ESM using thresholds based on EPA security directives; 2) information of facility security at the Headquarters location; and 3) information gained from analyzing more detailed ESM reports.

The field work was performed from September 1996 through March 1997. All work was performed in Washington, D.C. We conducted this audit in accordance with Government Auditing Standards (1994 revision) issued by the Comptroller General of the United States. Our audit included tests of management and related internal controls, policies, standards, and procedures specifically related to the audit objectives. Because this audit disclosed Agency-level weaknesses related to EPA's IRM Program, we also reviewed the OMB Circular A-123 evaluation process to determine why these weaknesses were not identified internally (see page 7). No other issues came to our attention which we believed were significant enough to warrant expanding the scope of the audit.

[2] High risk indicates a condition or control weakness which creates strong potential that disruptive intrusion could occur and even go undetected for some time; Moderate risk indicates that a compensating control has reduced the likelihood of intrusion or disruptive activity that such a condition or weakness could allow; Low risk means that all controls are in accordance with requirements and that there are no conditions which add risk to the facility or applications.

INFORMATION SECURITY REQUIREMENTS AND GUIDANCE

The responsibilities for information security at EPA are decentralized. The Office of Information Resources Management (OIRM) develops and defines the information security for the Agency. They disseminate the policies and provide some security training. However, each site with a LAN, whether it be a region, laboratory or program office must designate an ISO to be responsible for the overall security of the ADP facilities and applications processed there. In addition, for each LAN there should be a properly trained LAN Systems Administrator (SA) who is responsible for day to day implementation, maintenance, and monitoring of security for the LAN(s) they administer.

Office of Management and Budget (OMB) Circular A-130 is entitled “Management of Federal Information Resources.” Appendix III of this circular is entitled “Security of Federal Automated Information Systems.” This appendix details the required policy and guidance agencies must provide to ensure that automated systems have adequate security programs and documentation**.**

It establishes a minimum set of controls to be included in Federal automated information security programs; assigns Federal agency responsibilities for the security of automated information; and links agency automated information security programs and agency management control systems established in accordance with OMB Circular A-123. The Appendix revises procedures formerly contained in Appendix III to OMB Circular A-130 (50 FR 52730; December 24, 1985), and also incorporates requirements of the Computer Security Act of 1987 (P.L.100-235) and responsibilities assigned in applicable national security directives.

OMB Circular OMB Circular A-123 requires agencies to provide a feedback and reporting procedure to evaluate the integrity of Federal Programs for which they are responsible. This includes the management of its information resources. This circular specifically lists “Reviews of systems and applications conducted pursuant to the Computer Security Act of 1987 (40 U.S.C. 759 note) and OMB Circular A-130, "Management of Federal Information Resources" as information sources to be used in assessing and improving management controls OMB Circular A-123 also states that “the documentation for transactions, management controls, and other significant events must be clear and readily available for examination”.

EPA Directive 2100 - Information Policy Manual, Chapter 8, contains Agency security requirements policy. It iterates that EPA considers all of its information to be sensitive and that OMB Circular A-130 requirements for evaluating security controls should be followed. It also assigns responsibility for many related functions**.** EPA’s Information Security Program is OIRM’s responsibility while “Primary Organization Heads” are required to provide annual assurances that information resources are adequately protected using the OMB Circular A-123 process. It is this directive which specifies that: “Senior Information Resource Management Officials (SIRMO) are responsible for approving information security plans and certifying sensitive systems within their primary organizations;" and "Information Security Officers (ISO) are responsible for ensuring that comprehensive information security programs are in place for installations within their organizations." Guidance for implementation of these requirements is found in EPA's Information Security Manual (ISM) (Directive 2195) which has been undergoing revision.

Appendix A of EPA's Information Security Manual (ISM) dated October 23, 1995 was used for the development of the technical portion of EPA's Application Security Plan. The ISM complies with the guidance in OMB 90-08 and can be used. OMB Circular A-130, dated February 1996, states that until NIST publishes a new Federal Information Processing Standards (FIPS) on Security Plans, the appendix of OMB Bulletin 90-08 can be used as guidance for Application Security Plans. EPA's ISM is currently being updated to comply with the latest OMB Circular A-130 Appendix III. In the interim, the Chief Information Officer issued a memorandum summarizing the changes in the new Appendix III. That memorandum, dated April 3, 1996, stated that the ISM was being revised to comply with the new OMB requirements. Further, the new Agency guidance will require a consolidated document (i.e., a major application or general support system security plan) which will combine facility security, disaster recovery, along with application security. In response to our concerns, on February 21, 1997, EPA's National Program Manager for Information Security issued a draft NIST guide, *User Guide for Developing and Evaluating Security Plans for Unclassified Federal Automated Information Systems* as interim EPA guidance to the ISOs.

EPA's Management Integrity Guidance provides guidance and assigns responsibility for the Agency OMB Circular A-123 process. However, this guidance and Directive 2560 are out of date, because they both predate the latest OMB Circulars A-123 and A-130.

EPA Enterprise Technology Services Division (ETSD) Directives 310.01 through 310.13 and the LAN Operations Procedures (LOPS) Manual contain operational guidance and procedures regarding LAN standards. These sources contain chapters on LAN security.

SECURITY CONTROLS AT SMALL PURCHASE ELECTRONIC DATA INTERCHANGE (SPEDI) PRODUCTION SITES NEED IMPROVEMENT

Survey results revealed that security controls need improvement at all of the responding production SPEDI sites. The survey also indicates significant shortcomings in documentation of security controls at both application and LAN/facility level, as well as disaster recovery procedures and contingency planning. According to the survey, there is confusion concerning the need for security controls, security documentation, and the overall risk associated with SPEDI application. Five production sites issued no response to our survey by either the LAN SA or the ISO. Therefore, there is no assurance any of these five sites have designated the required security personnel; implemented adequate security measures; or produced security documentation required by OMB and the Agency. We also determined that information system security and security documentation were not being assessed as part of the Agency's OMB Circular A-123 process. Improvements were noted in implementation of security controls at the Headquarters site.

Inadequate Security Implementation At SPEDI Production Sites

None of the thirteen sites surveyed provided security documentation required for reasonable assurance that general controls are operating properly for the SPEDI application, in compliance with OMB and Agency requirements. Despite multiple requests[3], five production SPEDI sites did not respond to the survey. Therefore, there is no assurance that anyone is maintaining LAN or facility security at these sites.

1**.** Of the 13 sites surveyed, only 3 responded that there was a Security Plan for the SPEDI LAN, either in draft form or incorporated in the region's security plan**.** Of these positive responses, an actual copy was provided by only one site. Five other sites responded with a list of some security measures taken, but did not have either a LAN Support Security Plan or a Security Section of a General Support System Security Plan.**.**

2**.** Of the 13 sites surveyed, none were able to provide a copy of an Application Security Plan. A copy of a draft Security Plan for SPEDI has since been received under separate cover. Two sites responded that a draft security plan for the SPEDI application, as a whole, was being created by the ICMS development team. Five other sites responded with reasons why there was no such a plan.

[3] Requests made on October 15 and November 4, 1996.

3. Of the 13 sites surveyed, two sent Disaster Recovery Plans. Out of the remaining 11 sites, six responded that backups were being taken and being stored in a different location.

As part of the survey, we requested copies of the following three security documents for each site: 1) a Security Plan for the SPEDI LAN as required by OMB Circular A-130, and expanded by OMB Bulletin 90-08 and EPA's Information Security Manual (ISM); 2) an Application Security Plan for SPEDI, as required in OMB Circular A-130; and 3) a Disaster Recovery Plan for the SPEDI application, as detailed in OMB Bulletin 90-08 and EPA's ISM. The requested documents would satisfy either the previous or the February 1996 security control requirements. OMB Circular A-130 currently requires a Major Application Security Plan and a General Support System Security Plan for the application. The General Support System Plan should contain several components including a LAN Security Plan and Disaster Recovery Plan for the site processing the SPEDI application.

We received eight responses to this survey. Among the eight responding sites, there was reasonable assurance that some of the EPA required logical security was implemented via NetWare, but there were inconsistencies between individual sites. Although each of the eight responding sites performed security monitoring, the type of monitoring and the maintenance of monitoring reports or records was also inconsistent. All eight sites responded that they had adequate virus protection software and performed full and incremental backups.

OMB Circular A-123 Process Is Not Reporting Security Weaknesses

The OMB Circular A-123 Assurance Letters are not reporting incomplete security documentation or other security shortcomings which are security weaknesses. We reviewed six of the ten regional fiscal 1996 OMB Circular A-123 Assurance Letters, as well as the Assurance Letter issued by the Office of Administration and Resources Management (OARM). None of these letters reported incomplete security documentation as a control weakness, for either SPEDI or the regional sites. OMB Circular A-130 requires that management approve security plans at least every three years through the OMB Circular A-123 process. OMB Circular A-130 also specifies that security control weaknesses be reported as part of the Agency's OMB Circular A-123 annual review process. EPA's Information Security Program is relying on the managers of the individual sites and program offices to implement these Federal security requirements or to report information security weaknesses as part of OMB Circular A-123 process.

Corrective Actions And Compensating Controls Lower Risk At Headquarters Site

Our first test and analysis of logical security implementation at Headquarters SPEDI LAN (executed on 11-20-96) identified five 'high risk' conditions that severely downgraded or negated operating system security controls:

1. The number of accounts having the equivalence of 'supervisor'[4] exceeded the number allowed in EPA policy;
2. Several of these 'supervisory' accounts were inactive which increases the associated risk of misuse;
3. Agency-mandated password controls were negated by incorrect implementation of certain password features;
4. Some accounts allowed unlimited concurrent logins which greatly increases risk of undetected intrusion; and
5. Many powerful system files were duplicated.

In addition, our analysis identified the following six conditions as 'moderate' risk:

1. DCFC1's AUTOEXEC.NCF file did not remove the DOS operating system from the computer console or lock the console keyboard access[5];
2. Improper implementation of operating system intruder detection parameters;
3. Required password length was too short on some accounts;
4. Some accounts were not required to change passwords frequently enough;
5. Some accounts were allowed more than one concurrent login; and
6. Some accounts did not have the ability to change passwords.

Results of a second test (executed on 12-20-96) of the Headquarter's server revealed complete corrections to or significant improvements upon several conditions which had been designated as 'high risk' as a result of the first test. A walkthrough of the SPEDI LAN site at Headquarters also revealed that good physical security controls were in effect.

[4] Supervisor equivalence is assigned to a user account by the account SUPERVISOR. It has the same access rights as the original SUPERVISOR, which means that it can do anything to any file regardless of its contents or origin.

[5] This was initially downgraded from "high" to " moderate" risk because compensating controls limited physical access to the server.

Corrective actions and/or compensating controls scheduled or implemented will significantly reduce the level of risk to SPEDI at Headquarters. The level of risk has been reduced to a “moderate risk” in all but one instance. Duplicate files have been scheduled to be cleaned up and ESM monitoring software is scheduled to be installed on the server. The other high and moderate risk conditions have been corrected or addressed by a compensating control. However, the number of accounts with “supervisory” security equivalence are still not reduced to the level required by EPA policy. The number of such accounts was reduced to 8 but the Agency (LOPs and Directive 310.09) required limit is 3.

LACK OF APPROVED SECURITY PLANS CONSTITUTES CONTROL WEAKNESS

We consider the absence of management approved security plans for the SPEDI application and LANs to be a serious control deficiency, because there is a high risk of potential loss or manipulation of critical procurement data. The Agency also identifies it as a major system. The Information Systems Inventory (ISI) describes SPEDI as a Level II Information System, and this indicates that it is considered to be critical to each of the particular regions or contract management sites it serves. Although these sites are not in compliance with OMB Circular A-130 and Agency IRM security directives, the ‘assessable unit’ manager has not identified this as a serious internal control weakness. Therefore, top management was not reporting or initiating corrective actions through the Agency’s OMB Circular A-123 process.

The risk of disruption to SPEDI processing and loss of integrity of its data is increased due to security control weaknesses. Incomplete Security and Disaster Recovery provisions increase likelihood of exposure[6] of SPEDI LANs and the SPEDI application to an undesirable result. This could create disruption in service or loss of data integrity. Loss of data integrity could also hamper EPA’s ability to process payments for procurements. In fiscal 1996 SPEDI processed $44 million of Agency procurements.

SECURITY FOR SPEDI NEEDS INCREASED ATTENTION AT MANY LEVELS

Our survey revealed varied reasons for the inadequate amounts of security documentation and inconsistent implementation of security controls at the production SPEDI sites. Personnel at these

[6] An exposure is the probable result (such as logical or physical changes to processing programs or data which could render the application and/or the data it processes inaccurate or unavailable) of the occurrence of an adverse event.

sites were confused about EPA guidance to assist in the development of the required security documentation. There is also no coordinated overall security documentation for the SPEDI application for its production sites. Further, the survey indicated security personnel are confused about their responsibilities. In addition, not all ISOs from these sites have attended an EPA Security Conference which addressed the latest OMB and EPA guidance. Lastly, inadequate security documentation is not reported because the June 1994 Agency guidance, under the current OMB Circular OMB Circular A-123, allows Management to decide what to report.

Agency Policy Needs Updating

Agency-wide security policy and guidance, implementing the most recent OMB Circular A-130, have not been finalized. EPA management has taken a number of initial steps to publicize the latest changes to OMB Circular A-130. In April 1996, EPA management provided an Agency-wide security update summarizing Appendix III of the revised OMB Circular A-130. OIRM management also provided Agency-wide guidance for Rules of Behavior in June 1996. Management officials indicated that EPA has not updated guidance on System Security Plans because it is waiting for the National Institute of Standards and Technology (NIST) to issue revised security planning guidance as called for in the revised A-130, Appendix III. EPA's National Information Security Program Manager is currently revising EPA's guidance using the most recent draft of NIST's Federal guidelines for the development and evaluation of security plans, per the revised Appendix III. In February 1997, the Program Manager for Information Security provided copies of the Draft "User Guide for Developing and Evaluating Security Plans for Unclassified Federal Information Systems" to the ISOs. This provides interim Agency guidance based on current OMB Circular A-130 requirements.

At the time of our field work, there was no official SPEDI-specific guidance provided for the ISOs or LAN SAs at each site. There is a draft Integrated Contract Management System (ICMS) System Security Plan and Risk Assessment which covers SPEDI, but it has not yet been distributed to the production SPEDI sites. OAM management stated that the ICMS draft Security Plan and Risk Assessment includes: 1) an Application Security Plan; 2) a Security Plan for the SPEDI LANs; and 3) guidance for Disaster Recovery Plans at SPEDI sites. OAM management stated that these documents will also provide the guidance necessary for individual SPEDI sites to develop their own Facility and Disaster Recovery Plans. This is in keeping with the new OMB Circular A-130 requirements. These documents are being reviewed by the OARM Senior Information Resource Management Officer (SIRMO).

More Training Needed For ISOs And Other Security Personnel

Not all ISOs have received security training. EPA management conducted a security conference in August 1996. Attendees were provided with security training and guidance on Agency security documentation. In addition, in March 1997, OIRM conducted an ISO Forum to address similar security issues. However, not all ISOs were in attendance at these conferences. OMB Circular A-130 and EPA's ISM both require training for all employees based on their functions. They also require that ISOs be designated in writing. The non-responses to the survey provide no assurance that all production SPEDI sites have a properly designated ISO.

The survey indicated that personnel incorrectly believe: 1) SPEDI is a low risk system; 2) implementation of some security controls meets the requirement for security documentation; and 3) that SPEDI is not yet a production system**.** Few users and a low volume of transactions were conditions associated with low risk by respondents at some of the sites. In our opinion, SPEDI is a high risk system because: 1) it was used for authorization of approximately $44 million of purchases in fiscal year 1996 and will handle more in future fiscal years; 2) it is part of the Integrated Contract Management System; and 3) it is a manual feeder system for the Integrated Financial Management System. Therefore, it is necessary that adequate controls be in place to protect the integrity of SPEDI and its data**.** The responses of those sites viewing SPEDI as low risk indicate need for additional guidance or training to: 1) explain the potential for risk to appropriate personnel; and 2) require a more formal approach by developing a security plan and disaster recovery plan.

Agency OMB Circular A-123 Process Needs To Incorporate A-130 Requirements

Our audit noted that EPA's Resources Management Directive 2560, *Internal Controls*, dated June 12, 1987, is outdated and does not address the new requirements added by OMB Circular A-130 in February 1996. An Agency official stated that they are in the process of revising Directive 2560, but that completion is pending a reorganization of the Resource Management Division (RMD). RMD also indicated that the National Information Security Program Manager (i.e., OIRM) needed to provide assessment guidelines. EPA issued interim OMB Circular A-123 guidance under a memorandum entitled *Management Integrity Guidance*, dated June 1994. The interim guidance interprets OMB Circular A-123 as requiring a decentralized approach to reporting integrity weaknesses. Therefore, the OMB Circular A-123 process relies on the management of each 'assessable unit' to determine the integrity requirements of their programs within approved OMB and Agency guidance**.** The Assistant Administrators (AAs) and Regional Administrators (RAs) are also responsible for addressing OMB Circular A-130, OMB Circular A-123 and EPA's Management

Integrity Guidance. Agency Directive 2100 Chapter 8 assigns Information Security requirements to SIRMOs and ISOs, which are under the AAs and RAs.

Whereas 'assessable unit' managers should incorporate the Agency security requirements into their respective OMB Circular A-123 program reviews, our survey results indicated that the 'assessable unit' managers are confused about OMB Circular A-130 security plan requirements and related requirements identified for OMB Circular A-123. As a result, they are not identifying or reporting Agency security control weaknesses as part of the OMB Circular A-123 process.

In response to our interim comments, in February 1997, the National Information Program Manager sent a memorandum to the ISOs mentioning the need to evaluate information security as part of the OMB Circular A-123 process. This memorandum also requested information regarding the status of security plans for their applications or general support systems. A draft of "User Guidance for Developing and Evaluating Security Plans for Unclassified Federal Information Systems" was provided to assist the ISOs. The Information Resources Management Security Program has not established a separate feedback mechanism to ensure accountability regarding the status of Agency security plans because it relies on 'assessable unit' managers to identify and report Agency security control weaknesses under the OMB Circular A-123 process. EPA Directive 2100 states that the Primary Organization Heads should utilize the OMB Circular A-123 process to provide assurance on the information resources within their organization. Therefore, OIRM is dependent on the OMB Circular A-123 process to provide feedback on problems with Agency security plans.

LAN Consolidation Procedures Need Clarification

There are several reasons why proper security controls were not in place when we first tested the SPEDI LAN at Headquarters. The controls were not correctly established because the LAN SAs had not developed a security plan based on both EPA policy and SPEDI requirements. Subsequent to our field work, the ISO provided us a draft security plan for the Fairchild Consolidated Local Area Network. Also, prior to our evaluation, there was no monitoring software installed on the server (such as ESM), and NETWARE auditing features were not activated which could identify security settings. Management officials at Headquarters stated that they plan to obtain ESM software to monitor the LAN logical security controls. Management officials raised some additional, ongoing difficulties in establishing controls:

- Restricting users with supervisory\ access is difficult because our audit was performed after an Agency-mandated LAN consolidation which resulted in the server being shared with two other offices (Office of Grants and Debarment, Financial Management Division);

- As part of a server migration, many of the accounts on DCFC1 were copied from one server to the other without cleaning them up**.** This resulted in duplicate accounts or accounts with excessive privileges; and
- Ongoing software upgrades create many duplicate files.

Our audit of ETSD's Operational Directives 310.01 to 310.13 and LOPS Manual identified no established Agency guidance for LAN server sharing across multiple organizations.

RECOMMENDATIONS

1. We recommend that the Director for Information Resources Management finalize and implement Agency policies and guidance to assist 'assessable unit managers,' SIRMOs, and ISOs in the completion, establishment, and assessment of Application and General Support System Security plans, as required by OMB for fiscal 1997. We also recommend that continued training be provided to these personnel to better ensure completion of the Security Plans and their assessments.

2. We recommend that the Director for Planning, Analysis, and Accountability update Agency Integrity Guidance to comply with OMB Circular A-123, dated June 1995.

3. We recommend that the Director for Acquisition Management direct:

a. The Program Manager, Integrated Contract Management System within Headquarters Procurement Operations Division to:

(1) Coordinate with appropriate SPEDI ISOs the completion and approval of SPEDI (ICMS) Application and General Support System Security plans.

(2) Provide all production SPEDI sites interim guidance for developing a local Application Security Plan.

b. The SPEDI LAN System Administrator for Policy, Training, and Oversight Division's System and Information Management Branch to:

(1) Complete planned corrective actions to eliminate duplicate files.

(2) Obtain and install ESM software on the Fairchild Consolidated Local Area Network and monitor operational controls.

c. The ISO for Policy, Training, and Oversight Division's System and Information Management Branch to:

(1) Finalize the draft security plan for the Fairchild Consolidated Local Area Network.

(2) Obtain official guidance from EPA's National Information Security Program Manager regarding the number of supervisory accounts allowed when sharing a server, and implement the guidance into security maintenance and ESM monitoring practices.

AGENCY RESPONSE AND OIG EVALUATION

In summary, the Agency agreed with six of the eight recommendations in our draft report, partially agreed with one recommendation, and disagreed with one recommendation by asserting that corrective action had been sufficiently addressed through another program office's recent actions. To date, the Agency has taken a number of positive actions to correct the deficiencies. The report findings were directed to three distinct action officials and, therefore, we addressed their responses individually as follows:

In responding to the draft report, the Director for Information Resources Management agreed with recommendation 1 and provided details on planned and initiated corrective actions. OIRM is continuing to revise existing Agency policy and guidelines and recently developed new guidance for security plan development. On July 1, 1997, EPA's National Program Manager for Information Security distributed EPA Information Security Planning Guidance (dated June 17, 1997) to all ISOs. In addition, OIRM conducted training sessions for ISOs and SIRMOs, and consultation services are available to organizations in Headquarters and the Regions.

OIRM's response also indicates that ISOs will be responsible for providing SIRMOs with sufficient information to determine the adequacy of information security practices for systems under their purview. The response clearly states OIRM's dependence on the network of ISOs for awareness of and compliance with OMB A-130 requirements on Information Security Plans. In addition, the CIO recently issued a memorandum to EPA's Senior Resource Officials reiterating the need to review management controls pertaining to the security of Agency information as part of the on-going Integrity Act process.

In response to recommendation 2, the Acting Deputy Director for Planning, Analysis, and Accountability (OPAA) stated that this recommendation should be redirected to the Chief Information Officer (CIO) and asserted that recent CIO actions had satisfied the OIG's recommendation. We agree that the CIO's memorandum to EPA's Senior Resource Officials (SROs) and the Chief Financial Officer (CFO) partially addresses recommendation 2. The OIG recognizes that the actions of the CIO and OARM are two positive steps toward identifying Information Security as a potential control weakness and thereby raising the level of attention in the Agency as a critical internal control. However, these actions do not alleviate OPAA of responsibility for updating Agency-wide guidance and policies for the Management Integrity Program. Although individual Regional Administrators and Assistant Administrators may be responsible for interpreting how integrity guidance applies to their programs, outdated Agency guidance and policies should be updated to implement current OMB A-123 (June 1995) requirements.

The current OMB Circular A-123 promotes the integration of efforts to meet the requirements of the Integrity Act with other efforts to improve effectiveness and accountability. It recognizes the judgement of managers as a key component in assessing controls for their respective program(s). However, OMB Circular A-123 specifically states that 'other policy documents may describe additional specific standards for particular functional or program activites'. It also states that 'agencies need to plan for how the requirements of this Circular (A-123) will be implemented'. It goes on to say that 'a written strategy for internal agency use may help ensure that appropriate action is taken throughout the year to meet the objectives of the Integrity Act' and that 'absence of such a strategy may itself be a serious management control deficiency'. OIG believes that not having current integrity guidance and policies for EPA constitutes a serious management control deficiency. This situation increases the likelihood that the requirements of the Integrity Act will be misconstrued or ignored altogether. We believe that the Integrity Act's attempt to reduce unnecessary control processes or reporting requirements should not be interpreted by OPAA (or EPA) as a reduction or elimination of any General or Specific management control standards identified in other OMB Circulars. Until the existing EPA Integrity Act policy and guidance is updated, the OIG will recommend through the Integrity Act process that the lack of current policy and guidance be reported as a serious internal control deficiency. We revised recommendation 2 accordingly.

In their draft response to recommendation 3, the Director for Acquisition Management agreed with the primary findings regarding the improvement of security control at all of the production SPEDI sites and that documentation of security controls at both the application and LAN/facility level need to be developed.

In particular, OAM management described their plans to implement recommendation 3a.(1) and stated that they plan on using the draft guidance User Guide for Developing and Evaluating Security

Plans for Unclassified Federal Automated Information Systems in developing an Application Security Plan for the Integrated Contracts Management System (ICMS) family of applications, which includes SPEDI. A draft ICMS Application Security Plan is scheduled for completion no later than August 31, 1997, and OAM anticipates finalizing this plan by November 30, 1997. In addition, a draft General Support System Security Plan for the platform on which these applications operate has been submitted. Rather than expending effort on finalizing this plan for the short time that OAM will remain in the Fairchild Building, OAM management will continue working with the Office of Information Resources Management (OIRM) on a General Support System Security Plan for their new location, the Ronald Reagan Building.

In their draft response to recommendation 3.a(2), OAM stated that as sections of the ICMS Application Security Plan are developed, they will be distributed as interim guidance to the SPEDI operations sites for comments. OAM contended that because the same versions of the ICMS applications are used throughout the Agency, only one Application Security Plan would be necessary. However, they added that individual sites will be encouraged to incorporate appropriate sections of that plan into the local site's General Support System Security Plan. The ICMS Application Security Plan will include Disaster Recovery and Contingency Plans for the ICMS and SPEDI platforms and consolidated databases at Headquarters. The remote sites will be encouraged to prepare or verify the existence of local Disaster Recovery and Contingency Plans that include provisions for the ICMS applications.

In addition, OAM stated that the duplicate files had been eliminated and they had attempted to install the current version of Axent's OMNIGUARD Enterprise Security Manager Software on the Fairchild Consolidated LAN. These two corrective actions were initiated in response to recommendations 3.b(1) and (2).

OAM is currently developing a General Support System Security Plan for the Ronald Reagan Building. This plan will cover the ICMS applications and all other applications to be operated on the consolidated LAN. This action was initiated in response to recommendation 3.c(1). In response to recommendation 3.c(2), OAM also received guidance from the National Information Security Program Manager on how to establish and justify the number of supervisory accounts required to manage the Fairchild Consolidated LAN.

While OAM's response identified many planned and initiated corrective actions, we note that these actions are not yet fully complete. Therefore, these recommendation will remain as stated in the draft report. We made some editorial changes to the final report in response to OAM comments. However, we cannot justifiably delete statements equating absent survey responses to a lack of proper controls at the non-responding sites. We twice distributed our survey through the ICMS program manager to those sites where SPEDI was in production at that time. As five of these sites were non-responsive to both survey requests, no evidence was offered as to the existence of any logical or physical controls at the sites. Likewise, we do not find it necessary to make changes concerning training because training provided by OIRM is detailed both in the text of the report and earlier in the section for Agency response and OIG evaluation.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX I
Page 1 of 2

REPORT DISTRIBUTION

Office of Inspector General

Acting Inspector General (2410)

Assistant Inspector General for Audit (2421)

Principal Deputy Assistant Inspector General for Audit (2421)

Deputy Assistant Inspector General for Internal Audits (2421)

Deputy Assistant Inspector General for External Audits (2421)

Director, Financial Audit Division (2422)

EPA Headquarters

Acting Director, Office of Information Resources Management (3401)

Director, Office of Acquisition Management (3801F)

Acting Deputy Director, Office of Planning, Analysis and Accountability (2721)

Chief Information Officer (3101)

Director, Information Resources Management Planning Division (3402)

Agency Audit Followup Official (3101)
Attn: Assistant Administrator for Administration and Resources Management

Agency Audit Followup Coordinator (2710)
Attn: Audit Management Team

National Program Manager for Information Security (3402)

APPENDIX I
Page 2 of 2

Special Assistant, Office of Acquisition Management (3801F)

Audit Liaison (3102)
Attn: Office of Policy and Resource Management

Audit Liaison (3802F)
Attn: Office of Acquisition Management

Audit Liaison (3401)
Attn: IRM Policy and Evaluation Division

Audit Liaison (2721)
Attn: Office of Planning, Analysis and Accountability

Program Manager for Integrity (2721)
Attn: Office of Planning, Analysis and Accountability

Program Manager, Integrated Contract Management System (3801)

Information Security Officer
Attn: Policy, Training, and Oversight Division (3802F)

LAN Systems Administrator (3802F)
Attn: Policy, Training, and Oversight Division

Systems Accountant, Office of the Comptroller (3304)

Research Triangle Park, North Carolina

Security Officer, Enterprise Technology Services Division (MD-34)