Review of Information Systems Security
Report No. OIG-AMR-30-00-03

INSPECTOR GENERAL

NATIONAL LABOR RELATIONS BOARD

WASHINGTON, DC 20570

September 29, 2000

I hereby submit a *Review of Information Systems Security*, Report No. OIG-AMR-30-00-03. This review was conducted to determine whether automated information systems at the National Labor Relations Board (NLRB or Agency) are adequately safeguarded.

The Office of the Inspector General contracted with Cotton & Company LLP to conduct this review. The review was conducted using the General Accounting Office's *Federal Information System Control Audit Manual*. The manual provides guidance in evaluating entity-wide security program planning, access controls, application software development and change controls, segregation of duties, system software controls, and service continuity controls.

The Information Technology Branch administers security over the System 80 mainframe computer, Headquarters network, email, and network servers. Regional Offices administer security over their local network servers. The Finance Branch administers security over the three principle financial systems.

The entity-wide security program planning was not in conformance with Office of Management and Budget requirements. Policies, procedures, and standards to manage and guide agency information system security activities did not exist and reviews of general support systems or major applications to identify vulnerabilities, assess risk, and develop suitable cost-effective controls commensurate with identified risks were not performed.

Access controls over general support systems and financial systems need improvement. General support system weaknesses included a lack of written procedures to ensure that users' account privileges were properly established and assigned, and that security administrators were not fully trained and could not demonstrate a clear understanding of software security controls available and how to use them. Finance systems access control weaknesses raise significant concerns about the reliability, accuracy, integrity, and completeness of the information maintained in the systems. The weaknesses included key employees sharing a common user account and password. Additionally, the Finance Branch Chief, Fiscal Operations Chief and Program Analyst have excessive privileges that could enable them to execute unauthorized transactions.

Application software development and change control weaknesses included: a system development life cycle methodology has not been developed, which has contributed to system development and implementation delays; system development and program changes were not documented; controls to test, review, and approve program changes before updating software were not in place; and a complete inventory of applications and programs was not maintained.

The Finance Branch has not developed adequate segregation of duty controls to prevent one person from performing incompatible functions, such as entering and approving vendor payments. For instance, the Finance Branch Chief is the security administrator for two financial systems and is also responsible for processing transactions for payment and for making software program changes. With these privileges, the Chief has the ability to independently enter and approve payments. Also, segregation of duty controls over the Finance Branch Program Analyst were inadequate to ensure that only authorized activities occur. The Analyst is responsible for all software changes and maintenance to the financial systems and he can modify the data and output files. The Analyst's privileges also enable him to initiate transactions and modify data.

Service continuity controls over both financial and non-financial systems do not provide sufficient protection against the impact of a local or national disaster or significant business disruptions. The Finance Branch receives mainframe computer services through the National Institutes of Health, which has a continuity and recovery plan. NLRB is not covered by this plan and has not identified alternative backup and recovery procedures. The Information Technology Branch procedures are inadequate, primarily, because they store system back-ups onsite.

Recommendations addressing these findings can be found on pages 15 through 17 of this report. We recommend that the Director of Administration coordinate policy level steps, such as conducting a risk assessment, establishing an oversight committee, assigning security functions, and implementing training programs. We recommend that the Finance Branch Chief develop written procedures for software program changes and controls for the financial data systems. We recommend that the Information Technology Branch Chief develop procedures that cover new systems and program changes, existing control weakness, and information system recovery and service continuity.

An exit conference was held on August 14, 2000, with the Director of Administration, Information Technology Branch Chief and the Finance Branch Chief to discuss the findings and recommendations. A draft audit report was sent to these officials on August 21, 2000, for review and comment. They agreed with 12 of the 16 recommendations, and will develop an action plan within 60 days of receiving the final report. They disagreed with our recommendation to include the finance system in the hot-site recovery services; we concurred and deleted this recommendation. The comments are presented in entirety as an appendix to this report.

They mostly disagreed with three recommendations to segregate duties in the Finance Branch for three financial data systems. Their response and our comments are addressed on pages 17 through 19 of this report. We believe these recommendations are valid and, if not adopted, the Director of Administration should obtain concurrence from the General Counsel that the Agency is willing to accept the increased level of risk that results.

Jane E. Altenhofen
Inspector General

BACKGROUND

The National Labor Relations Board (NLRB or Agency) administers the principal labor-relations law of the United States, the National Labor Relations Act of 1935, as amended. The Act is generally applied to all enterprises engaged in interstate commerce, including the United States Postal Service, but excluding other governmental entities as well as the railroads and the airline industries. NLRB authority is divided by law and delegation. The five-member Board primarily acts as a quasi-judicial body in deciding cases on formal records. The General Counsel, like each Member of the Board, is appointed by the President, and is responsible for the issuance and prosecution of formal complaints in cases leading to Board decisions. The General Counsel has general supervision of the NLRB's nation-wide network of offices and is responsible for the Division of Administration. Approximately 30,000 charges of unfair labor practices and 6,000 representation petitions are filed with the NLRB each year.

The Division of Administration includes the following branches: Finance, Budget, Personnel, Procurement and Facilities, and Information Technology. The Information Technology Branch (ITB) is responsible for developing, implementing, and maintaining agency-wide information systems controls and security policies, procedures, and practices. The other four branches have specific responsibilities for software application and information systems controls and security.

For Fiscal Year (FY) 2000, the Agency was provided an appropriation of close to $206 million and authorized 1,947 full time equivalents to staff operations at Headquarters and 51 regional, subregional, and resident offices (field offices) and 3 Division of Judges satellite offices. The FY 2000 ITB budget was $12.2 million, an increase of $3.2 million over FY 1999.

In FY 1999, NLRB began a three-year information technology (IT) modernization program. Major priorities included installing and maintaining local and wide-area networks, installing new hardware, developing new application software or modifying existing software, and restructuring the organization to meet new and emerging IT needs. As of July 31 2000, NLRB's infrastructure consisted of approximately 2,000 Pentium personal computers (PCs) connected to Novell networks, 300 laptop computers, 1,500 printers, and a combination of desktop and network scanners. The Agency used two types of network operating software (Novell IntraNetware 4.11 and Windows NT) and had four different network configurations. The Headquarters network supported all users in the Headquarters building, except the Division of Judges. The Regional Office network supported 32 regional offices and 3 sub-regional offices. The Resident Office network supported 16 resident offices. The Division of Judges configuration supported judges at Headquarters and in three satellite offices. NLRB's network servers used Novell IntraNetware 4.11, which were connected to NLRB's wide area network. Windows NT servers were used to house the Case Activity Tracking System (CATS) databases. The infrastructure also inluded the Unisys System 80 computer that maintained both historical and current case records of the Casehandling Information Processing System.

NLRB obtains information processing services through Memorandums of Understanding with the National Institutes of Health (NIH) and the Department of Agriculture National Finance Center (NFC). NIH provides mainframe computer services to process NLRB's financial data and maintain the Financial Management Information Accounting System (FMIAS) software. NFC processes and maintains NLRB's payroll and personnel data and software.

Other significant software applications residing on the Headquarters and/or regional servers include Procurement Management Information System (PMIS), Microcomputer Accounting Data Entry (MADE) System, CATS, and Enforcement Litigation systems. MADE is a PC-based software package, developed by an outside contractor, which was used and maintained exclusively by the Finance Branch. MADE enables the Finance Branch's accounting technicians to create vendor payment files for uploading into FMIAS and Treasury's payment system. CATS resided only in ITB and the field offices.

ITB handles security administration of the System 80 mainframe computer, Headquarters network, email, and network servers. Regional offices handle security administration of their local network servers and perform tasks such as adding and removing users from NLRB's network.

The Finance Branch administers security of the FMIAS, MADE, and Backpay Trust Fund (Backpay) systems. The Finance Branch coordinates with NIH for granting access privileges to FMIAS. NIH administers the physical and logical security controls over FMIAS. The Finance Branch handles access security to Treasury's Electronic Certification System (ECS), which includes delegating privileges, entering information into ECS, and certifying and approving electronic payment files sent to Treasury. The Finance Branch coordinates with Treasury's Financial Management Services, which administers logical security controls of the ECS.

The Personnel Branch administers security of the Payroll/Personnel System and the Time and Attendance (T&A) System. The Personnel Branch sets up new users, assigns privileges, enters payroll and personnel information, and reconciles the biweekly T&A input files to payroll.

OBJECTIVES, SCOPE, AND METHODOLOGY

Cotton & Company LLP conducted this review to determine whether Agency automated information systems are adequately safeguarded. This included ascertaining whether NLRB's infrastructure was adequately protected and safeguarded and NLRB's security program (policy, procedures, and practices) complied with applicable Federal laws and regulations, specifically: Office of Management and Budget (OMB) Circular A-123, Management Accountability and Control, dated June 21, 1995; OMB Circular A-127, Financial Management Systems, updated June 10, 1999; and OMB Circular A-130, Management of Federal Information Systems, dated February 8, 1996. The security program was evaluated to: determine if it provided a secure environment; safeguarded and protected sensitive data; and ensured NLRB's financial data was reliable, complete, and timely. Personnel Branch controls were reviewed and assessed to determine if they adequately compensated for the control weaknesses in the Payroll/Personnel System and operating facility at NFC, identified by the Department of Agriculture, Office of Inspector General. NLRB's network and client server controls were evaluated against National Institute of Standards and Technology (NIST) requirements.

An initial risk assessment of the NLRB information systems and technology general control environment was performed to identify and evaluate the impact of control weaknesses on the overall IT environment, and the specific impact on each significant application. The risks and vulnerabilities of controls were re-evaluated during each system's review to determine the impact on previously considered effective controls. The logical, physical, and management controls were reviewed for the following systems:

- Network (Novell and Windows NT servers);
- FMIAS, MADE, and ECS;
- Backpay;
- PMIS;
- Enforcement Litigation System; and
- Payroll/Personnel System.

The evaluation included:

- Reviewing NLRB IS policies, procedures, practices, and business and IS plans and programs;
- Performing a walk-through of NLRB's physical facilities;
- Reviewing and observing NLRB personnel performing security administration activities, such as granting and removing access privileges to specific applications and databases; entering, modifying, and removing data; making and installing program changes; and maintaining network operating systems;
- Reviewing NLRB in-house backup and service continuity procedures for application and operating system software, telecommunications applications, and business and financial data;
- Reviewing and testing of users' email and FMIAS accounts, and
- Reviewing third-party information system control and security review reports for NIH and NFC data processing facilities.

We conducted the review of NLRB's information system security program in three phases:

- Planning;
- Internal control evaluation, analysis, and testing; and
- Reporting.

The approach was designed to obtain sufficient quantitative and qualitative information on NLRB's information security program plans, structure, standards, policies, procedures, and administration to determine the adequacy and effectiveness of the information systems security to safeguard NLRB hardware, software, and data. The approach provided sufficient information concerning NLRB's controls to provide reasonable assurance that the control structure and framework are suitable and commensurate with perceived risks and magnitude of harm resulting from these risks. The review specifically addressed the control requirements for each of the six information system security control areas discussed in the Federal Audit Executive Council Committee's *Auditing in a Paperless Environment*, dated September 1999.

The review included interviewing appropriate management and technical personnel, reviewing support documentation, observing system activities, and testing controls. For controls deemed not in place, we identified the risks and vulnerabilities and assessed the compensating controls used to mitigate risk.

We conducted the review using the guidelines published in the General Accounting Office's *Federal Information System Control Audit Manual* (FISCAM), dated January 1999. This manual covers the essential requirements for evaluating NLRB's information systems general controls and security plan, program, and procedures.

Our evaluation covered the following six FISCAM general controls categories.

- **Entity-wide security program planning** provides a framework for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's computer-related controls.
- **Access controls** limit or detect access to computer resources (data, equipment, and facilities), thereby protecting these resources against unauthorized modification, loss, and disclosure.
- **Application software development and change controls** prevent unauthorized programming or program modifications.
- **Segregation of duties** are policies, procedures, and an organizational structure established so one individual cannot control key aspects of computer-related operations, and thereby conduct unauthorized actions or gain unauthorized access to assets or records.
- **System software controls** limit and monitor access to the powerful programs and sensitive files that control the computer hardware and secure applications supported by the system.
- **Service continuity controls** ensure that, when unexpected events occur, critical operations continue without interruption, or are promptly resumed and critical and sensitive data are protected.

For each of these six categories, we reviewed and assessed the adequacy and effectiveness of controls in place to reduce risks, minimize exposures, and increase assurance. Wherever possible, FISCAM control techniques and suggested procedures were followed to facilitate our evaluation. In addition to FISCAM, specific standards suggested or required by NIST's *Federal Information Processing Standards* (FIPS) and industry best practices were relied upon. These included FIPS Publication 191, *Guideline for the Analysis of Local Area Network Security*; Windows NT Security guidelines published by the System Administration Networking and Security (SANS) Institute; NIST's *Generally Accepted Principles and Practices for Securing Information Technology System*; and NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, dated December 15, 1998. Our review did not include external or internal penetration testing or testing for unauthorized activities.

FINDINGS

The NLRB's information system security program, plans, policies, and procedures did not fully comply with OMB Circulars A-123, A-127, and A-130. NLRB's logical, physical, and management security controls are not adequate to: prevent unauthorized activities; provide reasonable assurance that financial assets are safeguarded; and ensure that systems provide complete, timely, reliable, and consistent information.

ENTITY-WIDE SECURITY PROGRAM PLANNING

A comprehensive program for security planning and management is the foundation of an entity's security controls and a reflection of senior management's commitment to addressing security risks. OMB Circulars A-123 and A-130 require agencies to: (1) periodically assess potential risks and controls over sensitive information and systems; (2) develop security plans that include a security management structure with clearly defined responsibilities; (3) develop, implement, and maintain an information system security program to ensure adequate security is provided for all agency information and systems; and (4) perform security awareness training, monitoring, and reporting.

NLRB has not undertaken reviews of its general support systems or major applications to identify vulnerabilities, assess risks, and develop suitable cost-effective controls commensurate with the identified risks. For example, NLRB has not performed a risk assessment of the IT infrastructure or its financial systems in the past 18 months. Additionally, it has not documented the results of any assessments that may have been performed in the past 3 years. Senior program management officials stated that they believe the information in the new CATS, Enforcement Litigation System, Backpay System, MADE, and FMIAS were adequately protected and secured. Management assertions were not, however, based on documented risk assessments or reviews to identify sensitive data. Thus, management could not demonstrate that its systems contained adequate levels of security and protection commensurate with the magnitude of harm that could occur, sensitivity level of the information contained within the system, or a defined level of acceptable risk for the systems or major applications.

ITB administered the information system controls and security for general support systems, which includes network servers, communication systems, and non-financial applications. NLRB's entity-wide information security program did not comply with OMB Circular A-130 requirements. Specifically, ITB did not have:

- Policies, procedures, and standards to manage and guide agency information system security activities;
- A system security plan consistent with guidance issued by NIST;
- Clearly assigned security responsibilities to individuals with sufficient knowledge and training to implement effective and efficient controls;
- Defined "rules of the system" concerning the use of, security within, and acceptable level of risk for the system;
- A security-awareness training program for employees and contract personnel concerning security responsibilities and "rules of the system";
- A formalized incident response program and team to ensure that actual or perceived security incidents and breaches are promptly and properly reported and investigated;
- Continuity of service program to recover and restore IT services in the event of a significant disruption to computer hardware, software, or communication systems;
- A security monitoring program to identify, investigate, and report on suspicious activities and to review, assess, and report to senior management on the effectiveness and efficiency of information infrastructure security controls; and
- A certification and accreditation program and process to authorize, in writing, the use of each general support system based on the implementation of its security plan before beginning or significantly changing system processing.

NLRB IT management stated they were aware of weaknesses and inadequacies with the IT security program, however, chose to place its resources and priorities on the development and implementation of the new infrastructure. This decision left current security vulnerabilities and weaknesses unresolved. NLRB management stated that it is currently in the process of hiring a full-time security officer, e-mail manager, and telecommunication specialist that should strengthen the IT environment. In addition, application systems are being installed on NT servers rather than Novell to enable the use of more advanced security controls.

Specific financial and programmatic impact resulting from entity-wide control weaknesses are discussed under applicable FISCAM assurance areas.

ACCESS CONTROLS

OMB Circular A-130 requires agencies to safeguard assets, data, and hardware from unauthorized activities. Thus, access controls should be designed and implemented to adequately restrict access to financial and sensitive non-financial data and applications to individuals for specific authorized purposes. Additionally, access controls should prevent or help detect unauthorized access to computer resources, and unauthorized modification or disclosure of data. ITB administers access control of the general support systems; the Personnel, Finance, and Procurement branches administer access control of their specific financial systems. Thus, the general support and financial systems access controls are addressed separately.

General Support Systems

Physical and logical access security controls over the network (the wide and local area networks) and communication systems need improvement. We identified the following access control weaknesses related to general support systems, non-financial applications, client servers, and the CATS database.

- Written procedures and guidance were not in place to ensure that users' account privileges were properly established and assigned. Procedures called for the security administrator to assign a new user to an existing user group based on the supervisor's request. In most instances, however, the supervisor was unfamiliar with what privileges were being assigned.

- ITB security administrators were provided Windows NT and Novell NetWare security training, however, they did not demonstrate a clear understanding and knowledge of security controls available or how to effectively implement them.

- ITB and the Personnel Branch have not established written procedures to inform the ITB security administrator of personnel changes, such as termination or transfer to another branch or location. We noted that users' accounts were not being removed or deactivated from the network, email, and other applications in a timely fashion.

- ITB security administrators have knowledge of all users' network identification (ID) codes and passwords, which permits impersonation of authorized users and performance of unauthorized activities. Security administrators do not need to know the users' network passwords for administration purposes. In addition, the physical security controls over the user access request forms, which contain ID codes and passwords, are weak. These documents are maintained in a locked desk drawer within ITB's general work area.

- Network security packages were not installed to automatically require users to change network or email account passwords periodically or to prohibit multiple sessions by the same user, as recommended by NIST. The frequency of changing passwords should be based on the system privileges extended to the user and the sensitivity of the system. For instance, users with access to financial systems with privileges to enter, alter, approve, and release financial transactions (obligations, expenses and payments) should be required to change their passwords every 60 to 90 days whereas, employees who only have a network/email account should be encouraged to voluntarily change their account passwords every 90 days but be required to change their password every 180 days. Security and network administrators should be required to change their password every 30 days.

- ITB had not installed Internet software applications, also known as filters, to block access to inappropriate or harmful Internet web sites.
- The network security administrator for the Novell and Windows NT used the same ID and password for each of the network administration server accounts. This is a weak security practice, because it permits complete access to all administrator network accounts and domains in the event the information becomes known to an unauthorized individual.
- ITB's remote access dial-in security controls were weak, and monitoring controls were not in place. ITB does not maintain an inventory of authorized users with remote access privileges. Remote access system (RAS) controls do not deactivate the user account after three failed attempts, although they do disconnect the incoming call. RAS did not generate a report of the failed attempts for review to alert security administrators of potential hacking attacks.

Financial Systems

The Finance Branch has not established adequate controls over data entry, processing, and maintenance of these systems. Control weaknesses raise significant concerns about the reliability, accuracy, integrity, and completeness of the information entered, processed, maintained, stored, and reported by these systems. Controls do not provide NLRB management with an adequate level of assurance on reported assets and financial records.

FMIAS is a mainframe computer system housed at NIH, but operated and maintained by the Finance Branch. At least five individuals within the Finance Branch have remote job entry privileges to authorize the daily run as well as generate reports. These individuals share a common user account and password. One of these individuals is the Finance Branch Chief, who is also the FMIAS security administrator and a FMIAS programmer. As a programmer, the Chief can allocate and restore files, change programs, and create and insert data.

Although the designed logical controls for FMIAS may be suitable for the information technology environment, the Finance Branch Chief's security administration privileges are unnecessary and present a potential risk for unauthorized activities to occur without detection. The Chief has access to and control over all reports generated by FMIAS, thus, is able to modify such reports to prevent detection of unauthorized activity. Additionally, sharing a common user account and password is a poor security technique and preempts FMIAS-designed system audit trails and features and those provided by the mainframe security package, Remote Access Control Facility. Shared user accounts and passwords prevent clear identification of the individual performing specific actions.

MADE is a PC-based software package, developed by a contractor, that enables the Finance Branch accounting technicians to create a vendor payment file. MADE produces files: to update FMIAS and generate vendor payments for transmission to Treasury. All Finance Branch personnel are assigned privileges to MADE.

The design of MADE creates potential risks and exposures for unauthorized activities, duplicate payments to vendors, and expenditures to exceed established obligations. Although MADE creates the vendor payment transactions, it does not retain cumulative balances of obligations, fund availability, or information about previous payments made to vendors. Management claims that this information is contained in FMIAS, and erroneous or improper vendor payments or payments exceeding the obligation or funds available may be discovered through reports generated by FMIAS. This process is not designed, however, to prevent overpayments or duplicate payments or payments being made to ineligible persons.

MADE logical controls are weak and poorly designed. The logical controls do not permit users to create their own unique password, known only to them; do not automatically mandate users to change their password; and do not require passwords to be configured with Alpha/numeric characters. We also noted excessive privileges given to individuals, particularly the Finance Branch Chief, Fiscal Operations Chief, and Program Analyst. The Chief stated that NLRB plans to convert MADE to Windows 2000 by March 31, 2001, at which time security controls to address the password concerns will be added.

The Finance Branch has inadequate controls to restrict the Program Analyst's access to the MADE software used to generate the daily transactions. The Analyst is solely responsible for maintaining the MADE software and has the ability to place the software into production.

The Finance Branch Chief's security administration duties and responsibilities are incompatible with other assigned duties and responsibilities. The Chief is the security administrator for MADE and FMIAS. As such, he is the only person with security administration privileges to add or remove users, assign privileges, and change user passwords. Through these privileges, the Chief has full knowledge of all users' account passwords; may create new accounts; may authorize, approve, and initiate transactions to both system. Through the Chief's duties, he is responsible for overseeing the reconciling of NLRB's fund balance with Treasury.

The Fiscal Operations Chief has the ability to initiate and approve transactions, perform manual batch verification to source documents and the payment file and perform the electronic certification function. Although he cannot release the payment file to Treasury, his existing privileges are excessive and could result in unauthorized activities. The Backpay system is a Microsoft Access database residing on a Headquarters server, that was developed by the Finance Branch Program Analyst. The system was developed to maintain a database of escrow accounts and record and generate backpay payment transactions to discriminatees. Regional offices provide the Finance Branch with payment instructions and a memorandum identifying each discriminatee's name, social security number, current address, and information regarding the nature of the payment and the amount of the employer Federal Insurance Contributions Act (FICA) tax contribution.

Finance Branch accounting technicians enter the information received from the Region into the Backpay database. Three accounting technicians have authorized privileges to this database; access however, is not restricted by passwords. Technically, all Finance and Budget Branch personnel with Microsoft Access installed on their PCs have access to the Backpay database. Accordingly, controls over the database are not sufficient to detect or prevent unauthorized disbursements and assure data is accurate and complete.

APPLICATION SOFTWARE DEVELOPMENT AND CHANGE CONTROLS

OMB Circulars A-127 and A-130 require agencies to establish controls to ensure that newly developed systems and program changes work as intended, meet user needs, and are authorized. These requirements are commonly referred to as the System Development Life Cycle (SDLC) methodology. The purpose of the SDLC is to (1) provide a framework for ensuring systems are designed, developed, and implemented to meet the needs and requirements of the agency; (2) ensure that systems work as anticipated; and (3) ensure that controls are built into the system before being placed into production. Additionally, the SDLC methodology provides the framework for controlling software changes to reduce the potential for unauthorized program changes. OMB Circular A-130 also requires agencies to maintain current system documentation. Further, OMB Circular A-127 requires that (1) systems be certified to ensure that adequate controls are built in; (2) systems process information completely, accurately, and reliably; and (3) reliance can be placed on system records. The NLRB's application software development and change controls had the following conditions and control weaknesses.

- A SDLC methodology has not been developed and implemented. The lack of controls contributed to the CATS development and implementation delays and implementation problems with the new procurement system.

- System development and program changes were not documented by either ITB or the Finance Branch. ITB has not developed programming procedures and controls to ensure program documentation adequately provide a knowledgeable person an understanding of the system.

- Controls to test, review, and approve program changes before updating the software were not in place. The

Finance Branch and ITB did not have written procedures and standards to ensure these activities are performed by the appropriate individuals.

- Software library controls, which transfer programs changes and enhancements from the operating (production) environment to the test environment and back into the production environment, were not in place to restrict programmer access to the production application and programs. Programmers made changes to software and moved changes into production without a third party being involved. This creates opportunities to enter unauthorized program changes for executing unauthorized activities.
- ITB did not maintain a complete inventory of applications and programs.

The review identified the following system development programming weaknesses with the Backpay system.

- Specific escrow account balances and the total number of accounts were not automatically reconciled and verified between Backpay and FMIAS. Management however, claims current manual reconciling practices are sufficient.
- Backpay was not programmed to identify, compute, and reconcile interest earned on Backpay escrow account balances invested in US Treasury marketable securities to FMIAS. The Finance Branch manually recorded interest into Backpay.
- Backpay was not properly programmed to ensure disbursements do not exceed current outstanding account balances or to ensure accounts are automatically updated and reconciled with FMIAS balances. In June, Backpay showed 6 accounts with negative balances totaling approximately $30,487. The Chief stated "this was caused by a programming error in Backpay, which management is aware of and is currently addressing."
- Field office and Headquarters compensating controls are not in place to minimize the Backpay programming weaknesses. Supporting documentation required by NLRB procedures and from General Counsel Memorandum OM 98-57, dated July 15, 1998, do not ensure that erroneous payments can be identified. Regions do not provide a complete and certified listing of discriminatees prior to payment. The Compliance Officer generates the listing of discriminatees from various documents under his control. This listing is not required to be certified by a second person and controls are not uniformly applied among the Regions. Reports of discriminatee payments made by Finance are sent to the Regions for their record keeping purposes. These reports are subject to potential modification because the database controls do not prevent alteration of Backpay payment records.
- Field office and Finance Branch management controls do not ensure that proper payments of FICA, owed by the respondents, are identified and held in reserve for payment to the US Treasury. Finance Branch management contends that FICA payments owed (in dispute) by the respondent may not be properly identified and held in reserve, resulting in non-payment of FICA. The Finance Branch identifies these accounts for reporting of the FICA taxes owed by the respondent to Treasury. According to NLRB instructions, field offices are required to prorate the amounts of Backpay owed to discriminatees based on the differential of total backpay owed versus the settlement amount, less (if not specified) the amount of respondents' FICA.
- Backpay is not programmed to ensure escrowed funds that are required to be returned to the respondent or to the US Treasury are properly identified and handled.

Weak application software development and change controls increase the risk of unauthorized modifications to applications, that applications contain inadequate or ineffective security controls, and that programming errors or modifications are not detected in a timely manner to prevent processing errors.

SEGREGATION OF DUTIES

OMB Circular A-130 requires agencies to establish controls that allow personnel to perform assigned duties, but prevent or minimize exposures associated with overriding security and internal controls. Further, OMB requires agencies to periodically assess potential risks and controls over sensitive information and systems to ensure these controls work. To help reduce the potential for unauthorized activities, the Finance Branch has an informal "rule of two" procedure that requires more than one individual to complete a financial transaction.

The Finance Branch has not developed adequate segregation of duty controls to prevent one person from performing incompatible functions, such as entering and approving vendor payments for disbursing and releasing the approved payment file to Treasury. The Finance Branch Chief is responsible for reconciling NLRB fund balance with Treasury and producing and circulating financial reports to NLRB management and other entities. These activities provide the Chief with the ability to remove unauthorized transactions or to modify account balances, thus enabling unauthorized activities to occur but not be detected. In addition, the Chief is the security administrator for the FMIAS and MADE systems, which is incompatible with his duties as Branch Chief.

Segregation of duty controls relating to the Finance Branch Program Analyst were inadequate to ensure that only authorized activities occur. The Analyst is responsible for all software changes, and can modify the MADE data output files, as well as initiate and modify transactions in the Backpay database. These responsibilities provide the Analyst with complete control of both the software and data. The Finance Branch has not established procedures to review and approve program changes made prior to placing the changed programs into production. This increases the risk of unauthorized software modifications that bypass security controls or unauthorized transactions being entered and processed by the application.

SYSTEM SOFTWARE CONTROLS

OMB Circular A-130 requires agencies to limit access to operating systems, system utilities, and production data and software and monitor the access and use of powerful operating system utilities. System software controls are intended to provide reasonable assurance that operating system-based security controls are not compromised and the system will not be impaired. Although we did not note any specific system control deficiencies, ITB can strengthen its controls and minimize risk by reducing the number of ITB personnel with "all" system privileges and implementing system monitoring tools.

The Finance Branch obtains mainframe computer services from NIH to operate and maintain FMIAS. NIH's external auditor reviewed NIH's mainframe facility system controls. The audit report did not identify any control weaknesses that would impact FMIAS.

SERVICE CONTINUITY CONTROLS

OMB Circular A-130 requires agencies to perform risk assessments of the impact of a local or national disaster or significant disruption to business operations and to develop disaster recovery and business continuity plans to address risks and minimize impact. NIST has developed requirements to assist agencies in developing and testing information systems and data processing backup and recovery procedures.

As stated earlier, NIH provides mainframe computer services to NLRB for FMIAS. Although the NIH data processing facilities have developed and tested a continuity and recovery plan, NLRB is not covered by the plan. In the event of a major disruption to its facility, NIH would reestablish operations at a hot-site facility. A hot-site facility is a fully functional computer facility that consists of the computer hardware, software, and financial data that enables NIH to completely restore FMIAS operation within a 24-hour period. The basic service agreement (Memorandum of Understanding) between NIH and NLRB, however, does not cover these services. To obtain this service, NLRB would need to renegotiate its agreement with NIH.

ITB has not established adequate recovery and backup procedures for the network, servers, systems, and files residing at Headquarters. Although ITB performs nightly backups of the network, Regional servers, and the Unisys System 80 computer, backup tapes are stored in the System 80 computer room. Storing backup tapes onsite is not effective, because, in the event of a fire or other significant disruption occurring at Headquarters facilities, the tapes would not be available to restore information system services. Because of the age of the System 80 computer and difficulties with obtaining replacement parts, ITB recognizes that this system would most likely not be restored in the event of disruption, such as a major hardware failure of the computer-processing unit. ITB is currently undertaking initiatives to move to a new platform. Management, however, has not performed an assessment of the information stored and maintained on this hardware to determine if the information is needed and should be included in a service continuity plan.

RECOMMENDATIONS

We recommend that the Director of Administration:

1. Coordinate with the Chairman and General Counsel to initiate immediate action to develop, fund, and implement an information system security program that complies with OMB Circulars A-123, A-127, and A-130 requirements. This includes conducting a risk assessment, and identifying and assigning sensitivity levels of the data commensurate with NLRB's mission and risk of improper release.

2. Coordinate with the Chairman and General Counsel to establish a senior management oversight committee to demonstrate senior management commitment and support of an effective and efficient security program and communicate committee desires.

3. Coordinate with the Chairman and General Counsel to establish procedures to monitor and report on the effectiveness and efficiency of the Agency's information system security program once it is implemented.

4. Assign the security administration functions for MADE and FMIAS to someone who does not have access to or control supporting documents, or to someone who does not have privileges to enter, approve, and execute transactions within these systems.

5. Institute an individual development training program to ensure technical training is provided to ITB and Finance Branch personnel responsible for implementing new technology including implementing and maintaining security systems.

6. Implement an annual security awareness-training program to ensure all NLRB personnel are annually informed of their information system security responsibilities.

7. Implement access controls over MADE, FMIAS and Backpay trust fund systems to restrict Program Analyst's and Chief's access to the application software and databases.

8. Reassign the Finance Branch Program Analyst's security administration functions for the Backpay system to a person who does not have access to or control of supporting documents or have privileges to enter data into Backpay.

We recommend that the Finance Branch Chief:

9. Develop written procedures to document, review, and test all software program changes made to the FMIAS, MADE, and Backpay systems.

10. Review the feasibility and cost of modifying the current MADE and Backpay systems to resolve the access and password control weaknesses.

11. Coordinate with the Division of Operations-Management Associate General Counsel to develop and implement controls for certifying payees and reconciling the Backpay trust fund.

We recommend that the ITB Chief:

12. Develop and implement a SDLC methodology to control the development of new systems and program changes.

13. Develop procedures to address access control weaknesses related to the general support systems.

14. Develop and execute the security administration program required by OMB Circular A-130 to include clearly defined security responsibilities, security monitoring and reporting, and developing and implementing a security-awareness training program.

15. Develop, implement, and test an information system recovery and service continuity plan for the System 80, network, and NLRB mission critical and financial systems.

MANAGEMENT'S RESPONSE AND OUR COMMENTS

NLRB management stated that this security review was conducted during its 3-year modernization period. As such, the findings and recommendations are, in most areas, consistent with those of the agency and complement activities underway or being planned. Management stated that it agrees with 12 of the 16 draft report recommendations, but disagrees with four in whole or in part.

Management's complete response to the draft report is in the appendix. Its response to the four recommendations with which it did not agree are summarized here, along with our additional comments.

RECOMMENDATION NO. 4

Management Response. Management does not agree on the need to reassign FMIAS and MADE security responsibility. It states that existing compensating controls are sufficient to negate weaknesses resulting from the Finance Branch Chief having security responsibility. Pursuant to recommendations by a joint team from OMB, Treasury, and NLRB's Inspector General, the Finance Branch Chief is not a certifying officer, has no budget authority, and thus cannot certify or authorize bills for payment. Although the Chief can enter, approve, and execute transactions, he cannot disburse funds without certifying officer approval. With control over FMIAS and MADE, the Chief and the Program Analyst can quickly fix problems to meet fiscal goals.

Comment. The Finance Branch Chief's function as security administrator is incompatible with other assigned duties. This situation could enable the Chief to circumvent or nullify existing controls, such as audit trails, files designed to detect unauthorized activities, or means to identify individuals performing unauthorized activities. In addition, the compensating controls that management considers sufficient are not outside of the direct influence of the Chief. Further, security administrator duties do not require highly specialized or technical skills and are not a normal or critical function of a finance branch chief. Management's comments about the OMB, Treasury, and NLRB Inspector General's 1992 review do not provide enough information to revise this recommendation. Management did not provide documentation to enable us to ascertain if system risks and control weaknesses identified in our report existed at the time of the review.

RECOMMENDATION NO. 7

Management Response. It is not practical to reassign the FMIAS, MADE, and Backpay system functions assigned to the Finance Branch Chief and Program Analyst. Compensating controls that have long been in place are sufficient to negate any internal control weaknesses related to FMIAS and MADE. Management agrees that identified weaknesses regarding Backpay should be addressed as noted in its response to Recommendation No. 8 and its agreement with Recommendation No. 11.

Comment. Access to production software and databases should be restricted to preclude unauthorized changes. It is not prudent or necessary for a programmer to have direct and unrestricted access to financial records and software; this presents an opportunity for unauthorized activities to occur without disclosure or detection.

RECOMMENDATION NO. 8

Management Response. Management agrees with the concerns addressed by the recommendation, but does not agree with the recommended solution. The Finance Branch Program Analyst needs to have complete access to the Backpay system to quickly process discriminatee payments. Management plans to develop procedures in response to Recommendation No. 11 that will eliminate weaknesses caused by the Program Analyst's complete access to the Backpay system.

Comment. The security administration function should be reassigned. Security administration activities are not compatible with those of a programmer or persons with privileges to enter data or control supporting documentation. We further recommend that NLRB provide the new procedures for our review and approval before they are implemented to ensure they address the weaknesses noted.

RECOMMENDATION NO. 12

Management Response. The cost of including FMIAS in NIH's hot-site recovery services is not warranted, because FMIAS does not need to be restored within 24 hours of a disaster. It can be down a week or two without significant impact. The only external report with a short deadline is the monthly Statement of Transactions report, which can be prepared using printed copies of disbursement schedules.

Comment. We agree that FMIAS hot-site recovery services may not be necessary; thus, we have eliminated the recommendation from the final report and renumbered remaining recommendations). FMIAS should, however, be included in the risk assessment and system recovery and service continuity plan addressed in Recommendation Nos. 1 and 15.

APPENDIX

UNITED STATES GOVERNMENT
National Labor Relations Board

Memorandum

To: Jane E. Altenhofen
Inspector General

From: Gloria J. Joseph
Director of Administration

Date: September 22, 2000

Subject: Draft Report "Review of Information Systems Security"

The IG Review was conducted during the Agency's three year modernization (FY1999 - FY2001). The findings and recommendations of the review are, in most areas, consistent with those of the Agency and complement those activities underway or being planned. We agree with 12 of the 16 recommendations, but disagree with four of them in whole or in part. Our response to the IG findings in each specific area of the review and the reasons for our disagreement on four recommendations are addressed below. As required, an action plan will be developed for the remaining recommendations within 60 days of receiving the final report.

ENTITY-WIDE SECURITY PROGRAM PLANNING

The findings and recommendations of the IG review in this area are consistent with those of the Agency. The NLRB was taking the initial steps toward an IT Security Program as the IG review was being conducted. An NLRB IT Security Officer is being hired to develop and implement an Agency IT Security Program under the CIO. The direction of this program will also address the findings and recommendations of the IG report.

ACCESS CONTROLS

The Agency is in the midst of a modernization and transition of both infrastructure and application systems. All the procedures, hardware, and software to provide strong access controls are not yet in place; however, the Agency agrees with the IG review that this should be done, and will be developing access control enhancements in FY2001. In addition to the technology, the Agency will have to address IT security policy and employee security responsibilities in developing and enforcing adequate access controls. This will be done as part of the implementation of the security program.

APPLICATION SOFTWARE DEVELOPMENT AND CHANGE CONTROL

An agency-wide SDLC is being developed. It is already in draft. The SDLC model being developed will address the IG review findings and recommendations on this topic. The model will address change control, and be applicable to all application software, including financial and other administrative systems.

SEGREGATION OF DUTIES

It is difficult (and we believe not necessary) for a small agency to justify and acquire IT personnel resources in the quantity required to provide separation of duties to the extent recommended in the IG review. The Agency understands the concerns of the IG review and believes the necessary separation of duties and controls are in place to ensure appropriate levels of security and financial responsibility for the systems maintained by the Finance Branch. Moreover, the current assignment of duties was the result of recommendations made by a joint team from OMB, Treasury and the NLRB's Inspector General when the Finance Officer installed FMIAS and MADE. The team recognized that there was not a complete separation of duties, but considered the remaining internal weakness inconsequential, given the compensating controls that were in place. According, we disagree with the following three recommendations about segregation of duties in whole or in part:

Recommendation 4 - We disagree with this recommendation. There is no need to reassign responsibility for FMIAS and MADE security. Existing compensating controls provide sufficient internal controls to negate the weakness which results from the Finance Branch Chief having responsibility for the security of FMIAS and MADE. Pursuant to the recommendation from the joint team, the Finance Branch Chief is not a certifying officer and has no budget authority and thus cannot certify or authorize bills for payment. Moreover, only the General Counsel and Director of Administration have authority to appoint a certifying officer, thus assuring adequate control of the overall system of payments.

The ability of the Finance Branch Chief to enter, approve, and execute transactions is not a significant internal control weakness, because he has no mean of disbursing funds without the approval of one of the four certifying officials of the Agency. His control over FMIAS and MADE enable the Agency to meet some of its primary fiscal goals, such as paying our customers promptly, providing accurate and timely internal reports to management officials, and submitting required external reports by the due dates. The external reports are prepared based exclusively on the data in FMIAS. The Finance Branch has consistently met these goals. A significant factor in being able to meet these goals is that the Finance Branch's Program Analyst and the Finance Branch Chief have been able to quickly fix any problems that have occurred.

Recommendation 7 - We disagree with this recommendation as it applies to FMIAS and MADE. This recommendation is substantially the same as Recommendation 4, with respect to FMIAS and MADE. Since the Finance Branch Program Analyst and the Finance Branch Chief are responsible for FMIAS, MADE, and the Backpay system, it is not practical to reassign these functions. We feel that compensating controls that have long been in place are sufficient to negate any internal control weaknesses that exist with regard to FMIAS and MADE. With respect to the identified internal control weaknesses regarding the Backpay system, we agree that it should be addressed, as we note in our response to

Recommendation 8 and as noted by our agreement to Recommendation 11.

Recommendation 8 - While we agree with the concerns expressed by the recommendation, we disagree with the recommended solution under the particular circumstances. The Finance Branch Program Analyst needs to have complete access to the Backpay system since he is responsible for creating and maintaining the software. The ability of the Finance Branch to quickly process payments to discriminatees, no matter how large the case, is important to Compliance Officers, the Division of Operations Management, and the Division of Enforcement Litigation. This quick response to unique cases is possible only because he has control of the Backpay system. However, the new procedures that we plan to develop in response to Recommendation 11 will eliminate internal control weaknesses concerning payments to discriminatees from the Backpay system caused by the Program Analyst's complete access to the Backpay system.

SYSTEM SOFTWARE CONTROLS

The IG review suggests reducing the number of people with access controls and using system monitoring tools. Modern equipment is being installed this year and next year. Until that modernization is complete, the procurement of tools is not cost effective or technically practical. We do not want to buy tools for the current systems when those tools will be obsolete next year. Also, the older equipment requires more manual intervention than the newer equipment. We do not want to divert resources to improve old systems to the extent that we cannot pursue replacing the old systems with new systems. The Agency does, however, agree with the IG in principle, and will address software control software and procedures in implementation of its modernized systems.

SERVICE CONTINUITY CONTROLS

Like many of the other findings and recommendations in the IG review, the Agency does not disagree with the IG review, but the current level of technology, limited budget, and replacement schedule must also be considered. The modern technology includes swappable drives for "hot swaps" and back-up servers are maintained for immediate deployment. Unisys was hired to develop alternatives to the failing System 80, and back-up systems and instructions are being deployed to the field offices. There is significant progress in the area of continuity controls and part of the new security program will include continuation of these improvements to minimize the risk identified in the IG review. However, we disagree with one of the recommendations in this area:

Recommendation 12 - We disagree with this recommendation. The Agency has determined that FMIAS does not need to be up and running in 24 hours after a disaster. It could be down for a week or two without any significant impact. The cost of having NIH include FMIAS in its hot-site recovery services is not warranted. The only external report that has a short deadline is the monthly Statement of Transactions (SF 224). It is due by the fifth workday after the end of the month. Even if FMIAS were down for those five workdays, the printed copies of the disbursement schedules would allow NLRB to prepare and submit the monthly SF 224 by the due date.