Audit of Case Activity Tracking System Security
Report No. OIG-AMR-33-01-02

INSPECTOR GENERAL

NATIONAL LABOR RELATIONS BOARD

WASHINGTON, DC 20570

August 1, 2001

I hereby submit an *Audit of Case Activity Tracking System Security,* Report No. OIG-AMR-33-01-02. This audit was conducted to determine whether the Case Activity Tracking System (CATS) was adequately safeguarded in field offices. This audit was also performed to meet requirements established by the Government Information Security Reform Act, for the Inspector General to perform an evaluation of the National Labor Relations Board's (NLRB) information security program and practices.

The Office of the Inspector General (OIG) contracted with Cotton & Company LLP to conduct this audit. Cotton & Company conducted the audit using guidelines published in the General Accounting Office's (GAO) *Federal Information System Controls Audit Manual,* dated January 1999. This Manual covers Office of Management and Budget (OMB) Circular A-130, Appendix III, *Security of Federal Automated Information Resources,* that identifies information systems security requirements and provides guidance for evaluating general information systems controls and the security plan, program, and procedures for major applications.

When evaluated against the Federal Information Technology Security Assessment Framework, NLRB's security cannot be rated as a Level 1, the lowest rating. This is based on the fact that NLRB does not have a formal documented and disseminated security policy. The Framework consists of five levels. Framework guidance notes that agencies should achieve Level 4 and ultimately Level 5.

NLRB has not completely implemented recommendations contained in OIG report *Review of Information Systems Security,* OIG-AMR-30-00-03, dated September 29, 2000. Unimplemented recommendations address several issues discussed in this report. We found that: a CATS security program and plan was not in place to manage and address security risks, access controls to CATS and to its network did not comply with OMB Circular A-130 and GAO's Internal Control Standards for general and application controls, the Information Technology Branch (ITB) did not provide network system administrators with adequate guidance and training to restrict access to system administration tools, and field offices were improperly storing backup tapes within the office rather than offsite. No problems were identified with either the CATS application program change controls or segregation of duties.

Recommendations addressing these findings can be found on page 8 of this report. We recommend that the ITB Chief: correct CATS access control design deficiencies and password configuration weaknesses to ensure compliance with National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS), develop a CATS security plan, perform a CATS security review that conforms with NIST FIPS, install security software that provides automatic timeout features and password-protected screensavers for all personal computers and develop procedures to ensure that system administrator tools and network privileges are properly restricted. He should coordinate with the Division of Operations-Management Associate General Counsel to develop and implement a field office business contingency and disaster recovery plan that includes developing procedures for securing backup tapes needed to implement recovery.

The Agency hired an information technology Security Officer on July 15, 2001. The Security Officer will be responsible for implementing recommendations made in the report *Review of Information Systems Security,* OIG-AMR-30-00-03, dated September 29, 2000.

An exit conference was held on June 21, 2001, with the officials from ITB and the Division of Operations-Management to discuss the findings and recommendations. A draft report was issued for comment on June 27, 2001. The ITB Chief submitted written comments on the draft report. He stated that the recommendations were consistent with ITB's assessment and that he would develop an action plan within 60 days of receiving the final report. Management's comments are presented in their entirety as an appendix to this report.

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 some other governmental entities, as well as the railroads and the airline industry.

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 Board Member, is appointed by the President and is responsible for issuing and prosecuting formal complaints in cases leading to Board decisions. The General Counsel has general supervision of NLRB's nationwide network of offices, through the Division of Operations-Management, and is responsible for the Division of Administration.

The Division of Administration, Information Technology Branch (ITB), is responsible for developing, implementing, and maintaining NLRB information system controls and security policies, procedures, and practices. Field office personnel are responsible for security administration of their Novell network servers.

In Fiscal Year (FY) 2001, the Agency was authorized 2,002 people at: Headquarters; 3 Division of Judges Satellite Offices; and 32 Regional, 3 Subregional, and 16 Resident Offices (field offices). The Agency's FY 2001 appropriation was more than $216 million. Approximately 30,000 charges of unfair labor practices and 6,000 representation petitions are filed with NLRB each year.

To support its mission, NLRB has developed an information technology (IT) infrastructure consisting of personal computers (PCs) and local servers connected to wide area networks that provide a communication linkage to the Headquarters' network. NLRB uses both Novell IntraNetware 5.1 and 4.11 and Windows NT network operating software.

The Case Activity Tracking System (CATS) is an integrated information system (IS) designed to collect, process, and maintain casehandling data; track active cases; and compile performance measurement data. NLRB initiated the

development of CATS in FY 1995. CATS resides exclusively on the Windows NT platform and is currently in the production phase at all field office locations.

OBJECTIVES, SCOPE, AND METHODOLOGY

Cotton & Company LLP conducted this audit to determine whether CATS was adequately safeguarded in field offices. This included determining if policies and procedures provided reasonable assurance regarding:

- Security program planning and management,
- Access controls,
- Application program change controls,
- Segregation of duties,
- Operating system security, and
- Service continuity.

This audit also included an assessment of NLRB's corrective actions taken in response to recommendations in the Office of Inspector General (OIG) report *Review of Information Systems Security* (OIG-AMR-30-00-03), issued on September 29, 2000.

Cotton & Company evaluated NLRB's:

- IS policies, procedures, practices, and business and IS plans and programs for CATS and the general control environment;
- CATS security documentation;
- In-house backup and service continuity procedures for the CATS application and data, network operating system software, and telecommunications applications; and
- Network and CATS security administration procedures and practices.

Cotton & Company conducted the audit in three phases: planning; internal control evaluation, analysis, and testing; and reporting.

The approach was designed to obtain sufficient quantitative and qualitative information about CATS security program plans, structure, standards, policies, procedures, and administration to determine the adequacy and effectiveness of controls to safeguard its software and data. The approach provided sufficient information to determine whether the CATS control structure and framework are suitable and commensurate with perceived risks and magnitude of harm resulting from these risks.

The audit included interviewing appropriate management and technical personnel, reviewing supporting documentation, observing system activities, and testing controls. Tests were conducted at NLRB Headquarters and at four field offices: Region 22, Newark; Region 9, Cincinnati; Region 25, Indianapolis; and Region 31, Los Angeles.

Cotton & Company conducted the audit using guidelines published in the General Accounting Office's (GAO) *Federal Information System Controls Audit Manual* (FISCAM), dated January 1999. This manual incorporates guidance in Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, Appendix III, *Security of Federal Automated Information Resources.* OMB Circular A-130, Appendix III, identifies IS security requirements and provides guidance for evaluating general information systems controls and the security plan, program, and procedures for major applications. CATS is a major application as defined by OMB and the Government Information Security Reform Act (GISRA).

This audit also included evaluating the information security program as required by GISRA and OMB Memorandum M-

01-08. To promote consistent reviews across government, OMB's memorandum suggests the use of the Chief Information Officer (CIO) Council's Federal Information Technology Security Assessment Framework to form the basis for the annual program review. NLRB's security program was evaluated using this assessment tool.

Both OMB's memorandum and the CIO Council's Framework suggest using FISCAM as audit guidance in evaluating internal control. For each of the FISCAM categories, we reviewed and assessed the adequacy and effectiveness of controls in place to reduce risks, minimize exposures, and increase assurance. Wherever possible, we followed FISCAM control techniques and procedures to facilitate our evaluation. As required by OMB Circular A-130, Appendix III, we assessed technical controls using National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publication 112, Password Usage. We also used GAO's Internal Control Standards for general and applications controls and for information and communication controls.

This audit was performed in accordance with generally accepted government auditing standards during the period March through June 2001.

FINDINGS

When evaluated against the CIO council's Framework, NLRB's security cannot be rated as a Level 1, the lowest rating. We found that NLRB has not implemented a majority of the recommendations contained in the *OIG Review of Information Systems Security* (OIG-AMR-30-00-03), issued September 29, 2000. Several issues discussed in this report address unimplemented recommendations from the September 29, 2000, report. We found that: a CATS security program and plan was not in place to manage and address security risks; access controls to CATS and to its network did not comply with OMB Circular A-130, Appendix III, and GAO's Internal Control Standards for general and application controls; ITB did not provide network system administrators with adequate guidance and training to restrict access to system administration tools; and field offices were improperly storing backup tapes within offices rather than offsite. No problems were identified with either the CATS application program change controls or segregation of duties.

INFORMATION SECURITY PROGRAM

NLRB's information security program cannot be rated as Level 1, the lowest possible rating. This is based on the fact that NLRB does not have a formal documented and disseminated security policy. We evaluated NLRB's information security program using the CIO council's Framework. This approach begins with the premise that all agency assets must meet the minimum-security requirements of OMB Circular A-130, Appendix III. To meet the CIO council's Framework rating of Level 1, a security program must include the following:

- A formally documented and disseminated security policy covering agency headquarters and major components. The policy may be asset specific.
- A policy that references most of the base requirements and guidance issued.
-

A security program can achieve a Level 1 rating if there is a formal, up-to-date, documented policy that establishes a continuing cycle of assessing risk, implements effective security policies including training, and uses monitoring for program effectiveness.

AUDIT FOLLOW-UP

NLRB has only fully implemented 4 of 15 recommendations contained in the OIG *Review of Information Systems Security* (OIG-AMR-30-00-03), issued September 29, 2000. As a result, NLRB's IS security program continues to be in substantial non-compliance with OMB Circular A-130, Appendix III. NLRB's logical, physical, and management security controls are not adequate to prevent or detect unauthorized activities; provide reasonable assurance that information system data are safeguarded; and ensure that systems provide complete, timely, reliable, and consistent

information.

The Agency's action plan, dated November 29, 2000, anticipated implementing most recommendations by September 30, 2001. Included in this plan was the hiring of an IT Security Officer by March 31, 2001. The Agency selected an IT Security Officer who is scheduled to report for duty on July 15, 2001. The IT Security Officer would likely be responsible for implementing many of the recommendations. Implementation of corrective action should not be delayed. The status of corrective actions from the OIG *Review of Information System Security* (OIG-AMR-30-00-03) is included as an attachment to this report.

CATS SECURITY PROGRAM PLANNING

A CATS security program and plan is not in place to manage and address security risks. OMB requires an agency to implement and maintain the following controls for major applications:

1. **Responsibility for Security.** Assign responsibilities for security for each system to a management official knowledgeable about the information and process supported by the application and in the management, personnel, operational, and technical controls used to protect it.

2. **Application Security Plan.** Plan for adequate security of each major application, taking into account the security of all systems in which the application will operate. The security plan should be consistent with guidance issued by NIST. OMB Circular A-130, Appendix III, requires security plans to have the following:

a. **Application Rules.** Establish a set of rules for use of and behavior within the application

b. **Specialized Training.** Ensure that all individuals receive specialized training focused on their responsibilities and the application rules.

c. **Personnel Security.** Incorporate controls such as separation of duties, least privilege, and individual accountability into the application.

d. **Contingency Planning.** Establish and periodically test the capability to perform agency functions supported by the application in the event of failure of its automated support.

e. **Technical Controls.** Ensure that appropriate security controls are specified, designed into, tested, and accepted in the application in accordance with appropriate guidance issued by NIST.

f. **Information Sharing.** Ensure that information shared from the application is protected appropriately and comparable to protection provided when information is within the application.

g. **Public Access Controls.** Where an agency's application promotes or permits public access, add additional security controls to protect the integrity of the application and the confidence the public has in the application.

3. **Review of Application Controls.** Perform an independent review or audit of security controls in each application at least every 3 years. Consider identifying a deficiency pursuant to OMB Circular A-123, Management Accountability and Control, and the Federal Managers' Financial Integrity Act if there is no assignment of security responsibility, no security plan, or no authorization to process for a system.

4. **Authorize Processing.** Ensure that a management official authorizes in writing the use of the application by confirming that its security plan as implemented adequately secures the application.

ITB administers CATS IS controls and the general control environment consisting of network servers and communication systems. ITB has not accomplished the following specific OMB Circular A-130, Appendix III, requirements:

- Policies, procedures, and standards to manage and guide CATS security activities.

- Clearly assigned security responsibilities both within CATS and between CATS and the general control environment.

- A CATS security plan, containing all the requirements stated above in 2.a. through g., including a security awareness training plan for CATS.

- A review of CATS control addressing its use, security, and acceptable level of risk.

Additionally, the Division of Operations-Management and ITB did not perform a review that conforms to NIST FIPS Publication 102, *Guidelines for Computer Security Certification and Accreditation*, to ensure that CATS met OMB Circular A-130, Appendix III, IS requirements before placing CATS into production in field offices.

ACCESS CONTROLS

NLRB access controls to CATS and its network do not comply with OMB Circular A-130, Appendix III, and with GAO's Internal Control Standards for general and application controls. ITB did not design and implement sufficient security controls to adequately protect CATS software and data. Specifically, CATS password configurations did not consist of alpha, numeric, and special characters and have eight or more characters, as prescribed by NIST FIPS Publication 112. CATS access security features did not automatically prompt users to periodically change their passwords, encrypt password files, and preclude concurrent log-on sessions.

Further, ITB did not design timeout features and password-protected screensavers into CATS or install these features on the Windows Network or on PCs. These features are designed to automatically log off users for inactivity or lock a PC to prevent unauthorized activities from being performed while an employee is away from the workstation.

ITB has taken little action in response to network physical and logical access security control weaknesses identified in OIG *Review of Information Systems Security* (OIG-AMR-30-00-03), issued on September 29, 2000. The following access control weaknesses related to the Novell network continue.

- The Novell system security administrator is not properly maintaining user accounts by removing user accounts of terminated employees in a timely manner. The administrator is not maintaining an accurate and complete list of authorized users.

- The ITB security administrator has knowledge of all user network ID codes and passwords, which permits impersonation of authorized users and performance of unauthorized activities.

- Network security packages were not installed to automatically require users to change network or email account passwords periodically as recommended by NIST.

OPERATING SYSTEM SECURITY

ITB did not provide network system administrators with adequate guidance and training to restrict access to system administration tools. System administrator tools were not properly protected to prevent unauthorized use of powerful network privileges such as creating, deleting, or modifying accounts. OMB Circular A-130, Appendix III, requires limiting access to operating systems, system utilities, and production data and software. It also requires that agencies 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 a system will not be impaired.

SERVICE CONTINUITY CONTROLS

Field offices were improperly storing backup tapes within the offices rather than offsite. OMB Circular A-130, Appendix III, 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. NIST recommends storing backup and recovery tapes offsite or in a fireproof container onsite.

RECOMMENDATIONS

Several weaknesses were identified in this report and were also identified in the OIG *Review of Information Systems Security* (OIG-AMR-30-00-03): lack of a security program, need for training, need to strengthen access and software controls, and need for disaster recovery procedures. On November 29, 2000, the Director of Administration provided us with an action plan to correct identified deficiencies. Most of those actions are scheduled to be complete by September 30, 2001. Weaknesses in this report that were addressed in the prior report will be monitored through the audit follow-up process. Recommendations open for more than one year will be reported in the OIG semiannual report to Congress. It is imperative that the Agency takes immediate action on those recommendations to be in compliance with the basic requirements of GISRA. We have the following new recommendations.

We recommend that the ITB Chief:

1. Correct CATS access control design deficiencies and password configuration weaknesses to ensure compliance with NIST FIPS Publication 112.

2. Develop a CATS security plan that complies with OMB Circular A-130, Appendix III, requirements for major applications and is commensurate with management's defined level of risk for the CATS application.

3. Perform a CATS security review that conforms to NIST FIPS Publication 102.

4. Install security software that provides automatic timeout features and password-protected screensavers for all PCs.

5. Develop procedures to ensure that access to system administrator tools and network privileges is properly restricted.

6. Coordinate with Division of Operations-Management Associate General Counsel to develop and implement a field office business contingency and disaster recovery plan, including developing procedures for securing backup tapes needed to implement recovery.

EXHIBIT

Status of Proposed Management Corrective Actions in Response to Report No. OIG-AMR-30-00-03 Recommendations

Recommendation 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 commensurate with NLRB's mission and risk of improper release.

Action Plan	Status
1. Hire IT Security Officer.	1. Partially complete. An IT Security Officer is scheduled to begin work July 15, 2001.
2. Independent IT security assessment.	2. Partially complete. ITB hired GSA (May 9, 2001) to perform the network security assessment, which should be

completed within 60 days.

Recommendation 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.

Action Plan	Status
1. Document, distribute, and brief agency officials as necessary on the NLRB Security Program.	1. No action taken. This will be done after a risk assessment is completed.

Recommendation 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.

Action Plan	Status
1. Make IT security a project in the IT Operating Plan.	1. Partially complete. The CIO has been directed to develop a monitoring system to keep the Chairman and General Counsel informed of security issues and provide a report during the budget process. This recommendation can not be fully implemented until the security program is in place.

Recommendation 4: Assign the security administration functions for Microcomputer Accounting Data Entry (MADE) and Financial Management Information Accounting System (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.

Action Plan	Status
1. Select ITB Security Administrator (for MADE and FMIAS).	1. Complete.
2. Develop and implement access control procedures.	2. Complete.

Recommendation 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.

Action Plan	Status
1. Include new technology and IT security in the individual development plans (IDP) of appropriate IT and Finance employees.	1. No documentation was provided to support this action. See CATS Security Program Plan finding on page 5.

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

Action Plan	Status
1. Included in response to recommendation 14.	1. See recommendation 14 for status.

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

Action Plan	Status
1. Select ITB Security Administrator.	1. Complete.
2. Develop and implement access control procedures.	2. Complete.

Recommendation 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.

Action Plan	Status
1. Management will develop procedures to eliminate this weakness.	1. Complete. See recommendation 11.

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

Action Plan	Status
1. Use SDLC methodology in implementing software program changes.	1. Partially complete. A draft SDLC methodology is being used. The final SDLC plan, however, has not been approved and implemented.

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

Action Plan	Status
1. Convert MADE system from DOS to Windows.	1. Partially complete. The Finance Branch is taking steps to convert system.
2. Correct password control concern in MADE.	2. Partially complete. The Finance Branch is taking steps to convert system.
3. Correct password control concern in Backpay system.	3. No documentation was provided to support this action.

Recommendation 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.

Action Plan	Status
1. Discuss new procedure at Compliance Conference for processing of Backpay checks.	1. Complete.
2. Begin implementation.	2. Complete.

Recommendation 12: Develop and implement an SDLC methodology to control development of new systems and program changes.

Action Plan	Status
1. Develop NLRB SDLC methodology.	1. Partially complete. A final SDLC methodology has not been approved and implemented.
2. Incorporate SDLC methodology in all new software development.	2. Partially complete. ITB is using its draft SDLC.
3. Use SDLC methodology in maintenance and change of existing systems.	3. Partially complete. ITB is using its draft SDLC.

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

Action Plan	Status
1. Develop system plans and priorities.	1. No action taken.
2. Develop access control procedures.	2. Partially complete. See the CATS Access Control finding on page 6.
3. Install infrastructure control technology.	3. Partially complete. See Recommendation 1. Full completion requires FY 2002 funding.

Recommendation 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 development and implementation of a security-awareness training program.

Action Plan	Status
1. Hire IT Security Officer.	1. Partially complete. An IT Security Officer is scheduled to begin work July 15, 2001.
2. Create a security program that meets A-130 requirements.	2. Partially complete. See Recommendation 1. This will be completed by the IT Security Officer.
3. Complete Security Training Program Development.	3. Partially complete (same as above).

Recommendation 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.

Action Plan	Status

1. Network security hardware and software installed.	1. No action taken.
2. Mission Critical Systems backup and continuity implemented.	2. No action taken. See CATS Service Continuity Controls finding on page 8.
3. Replace the System 80.	3. Partially complete. Waiting for full implementation of CATS.

APPENDIX

UNITED STATES GOVERNMENT
National Labor Relations Board

Memorandum

TO: Jane E. Altenhofen
Inspector General

FROM: Louis B. Adams
Chief Information Officer (CIO)

DATE: June 28, 2001

SUBJECT: Draft Report "Audit of Case Activity Tracking System Security"

The six recommendations in the audit are consistent with our assessment. We will develop an action plan for them within 60 days of issuance of the final audit.

Attachment

cc: Director of Administration