Review of Information Security at the Railroad Retirement Board
Report No. 02-04, February 5, 2002

EXECUTIVE SUMMARY

This report presents the detailed results of the Office of Inspector General's (OIG) review of information security at the Railroad Retirement Board (RRB) which was performed pursuant to the requirements of the Government Information Security Reform Act. The OIG's summary findings were submitted, in the prescribed format, to the Chair of the Railroad Retirement Board for transmittal to the Office of Management and Budget. The full text of that document is presented in Appendix I to this report.

The RRB administers the retirement/survivor and unemployment/sickness insurance benefit programs for railroad workers and their families under the Railroad Retirement Act and the Railroad Unemployment Insurance Act. The RRB paid out over $8 billion in benefits during fiscal year 2001.

Our review disclosed weaknesses in most areas of the RRB's information security program. Significant deficiencies in program management and access controls make the agency's information security program a source of material weakness in internal control over financial reporting.

Access controls cannot be considered fully effective due primarily to inadequacies in password management. Our review identified numerous password management weaknesses in the mainframe, local area and wide area computing environments. The RRB's most notable problem is the agency's inability to police and enforce its recently adopted policy requiring the use of more complex password configurations. Other weaknesses observed during this review included: passwords that never expire, inactive, duplicate accounts, separated employees and former contractors whose information system privileges had not been revoked.

The overall effectiveness of the RRB's information security program has been undermined by a lack of training among key personnel. Employees with decision-making responsibility for information security have not had adequate formal training in its theory, principles and practice. In addition, the information security program lacks a strong security framework with a central management focal point. These two deficiencies are the underlying cause of many other control problems identified during the audit.

Our report also cites the agency for:

- weaknesses in the security planning and evaluation process;
- inadequacies in the design of controls intended to restrict individual privileges to the minimum required by their employment; and
- a lack of documentation for some security-related activities.

We have made specific recommendations for corrective action to strengthen controls in the areas of weakness identified by the audit. In their response to the draft audit report, the Bureau of Information Services concurred with most of the OIG's recommendations and stated that many had already been implemented. The full text of management's response is presented in Appendix III to this report.

INTRODUCTION

This report presents the results of the Office of Inspector General's (OIG) review of information security at the Railroad Retirement Board (RRB).

BACKGROUND

The RRB administers the retirement/survivor and unemployment/sickness insurance benefit programs for railroad workers and their families under the Railroad Retirement Act (RRA) and the Railroad Unemployment Insurance Act (RUIA). These programs provide income protection during old age and in the event of disability, death, temporary unemployment or sickness. The RRB paid out in excess of $8 billion in benefits during fiscal year (FY) 2001.

The RRB's information system environment consists of two general support systems and seven major application systems. The two general support systems are the data processing system, which supports all mainframe computing activity, and the end-user computing system, which supports the agency's local (LAN) and wide (WAN) area networks.

The major application systems correspond to the RRB's critical operational activities: payment of benefits, maintenance of compensation and service records, administration of Medicare entitlement, financial management, personnel/payroll, and the RRB's financial interchange with the Social Security Administration. Each application system is comprised of one or more programs.

The Office of Management and Budget (OMB) has published guidance to assist Federal managers in meeting the management control and computer security requirements of the Computer Security Act of 1987, Chief Financial Officers Act of 1990, and the Clinger-Cohen Act of 1996. OMB Circular A-123, "Management Accountability and Control," dated June 21, 1995, provides guidance on improving the accountability and effectiveness of Federal programs and operations by establishing, assessing, correcting, and reporting on management controls. OMB Circular A-130, "Management of Federal Information Resources," Appendix III dated November 30, 2000, establishes policy for the management of Federal information resources. OMB Circular A-130, Appendix III 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 with agency management control systems established in accordance with OMB Circular A-123.

The RRB has set forth agency-specific information security requirements in its administrative circulars: Circular IRM-7, "Security Plans for Information Technology Systems," dated May 22, 2000; IRM-8, "The Information Security Program of the

Railroad Retirement Board," dated July 18, 2001; and IRM-11, "Security for Automated Systems," dated June 17, 1994.

IRM-8 delegates authority to administer the agency's information security program to the Chief Information Officer. The Chief Information Officer is also the director of the RRB's Bureau of Information Services and is responsible for administration of both data processing and end-user computing as well as in-house systems development. In August 2001, the RRB appointed a new Chief Information Officer, filling a position that had been vacated the previous April.

On October 30, 2000, the President signed into law the FY 2001 Defense Authorization Act (P.L. 106-398) including Title X, subtitle G, "Government Information Security Reform (The Security Act)."[1] The Security Act requires annual agency program reviews, annual Inspector General security evaluations, an annual agency report to the Office of Management and Budget (OMB), and an annual OMB report to Congress.

The full text of the OIG's report to OMB is included as Appendix I to this report.

OBJECTIVES, SCOPE AND METHODOLOGY

The scope of this review was information system security at the RRB during May through September 2001.

The objective of this review was to fulfill the requirements of the Security Act by performing an evaluation of the RRB's information system security program and practices including tests of the effectiveness of security controls in an appropriate subset of agency systems.

In order to accomplish our objectives, we:

- reviewed laws, regulations, management control reports, policies, procedure and security planning documents;
- reviewed security incident reports, problem logs, and prior audits;
- interviewed staff and management with significant security responsibilities, such as system administrators;
- assessed agency compliance with OMB requirements for security, disaster recovery and contingency planning;
- reviewed mainframe global security settings and software rules controlled by Computer Associates' Access Control Facility (ACF2), a commercial data security product;
- obtained and reviewed a listing of inactive mainframe user accounts;

[1] This legislation is also referred to by the acronym "GISRA."

- tested a random sample of 120 agency employees to determine whether existing controls had been effective in ensuring that all mainframe accesses had been authorized, all authorizations had been documented and access rights had been restricted to the requirements of each user's job;[2]
- reviewed the security settings within the Federal Financial System (FFS) to assess the effectiveness of change-logging as implemented for that application.
- tested a non-random sample of 89 users of the PAR system to determine whether their application-level privileges had been restricted to the requirements of their employment;[3]
- reviewed the data center access privileges of individuals to determine whether their key cards appropriately restricted access to the minimum required by the cardholders employment;
- tested a non-random sample of 9 systems development projects for compliance with applicable policy and procedure;
- tested a non-random sample of data tapes stored off-site for timely return;
- obtained and analyzed a listing of LAN/WAN accounts; and
- reviewed the network account identifiers and status for a non-random sample of 42 LAN/WAN users.

We limited our evaluation of security for the end-user computing general support system to inquiries of LAN/WAN management, analysis of the user account population and detailed tests of selected user accounts. Our initial interviews with management identified weaknesses in the security provisions for the LAN/WAN system. These findings, discussed in detail beginning on page 14 of this report, indicated that additional detailed testing would not have furthered the objectives of this review.

In performing this review, we considered prior OIG audit findings and recommendations as well as third-party evaluations of information security at the RRB conducted at the request of the OIG:

- "Information Systems Security Assessment Report," Defensive Information Operations Group, National Security Agency, June 2000;
- "Site Security Assessment," Blackbird Technologies, Inc., July 20, 2001; and
- "Security Controls Analysis," Blackbird Technologies, Inc., August 17, 2001.

[2] The sample of 120 employees was drawn from the population of agency employees who were authorized users of the mainframe general support system or had been assigned an electronic mail address on the LAN/WAN general support system.

[3] The sample of 89 users of the PAR system was drawn from the population of individuals who had access privileges other than "Read Only."

A summary of the findings of Blackbird Technologies, Inc. is presented in Appendix II to this report.

Our work was performed in accordance with generally accepted government auditing standards as applicable to the audit objectives. Fieldwork was conducted at RRB headquarters during May through October 2001.

RESULTS OF REVIEW

Information security is an area of material weakness in internal control over financial reporting.

The present information systems security program does not reduce to a relatively low level the risk that misstatements, in amounts material in relation to the financial statements, could occur but not be detected within a timely period by employees in the normal course of performing their assigned functions.

Our review disclosed weaknesses throughout the RRB's information system security program. The most significant weaknesses relate to program management and access controls. Program management has been significantly undermined by a lack of training among key personnel. Access controls cannot be considered fully effective because of the numerous weaknesses in password management in both the mainframe and LAN/WAN computing environments.

The inadequacies in password management and training identified during our review place the RRB's financial information at risk of unauthorized modification or destruction, sensitive personal information at risk of inappropriate disclosure, and critical operations at risk of disruption. As a result, information system security is an area of material weakness in internal control over financial reporting.

In addition, security responsibilities are fragmented throughout the agency. The lack of a strong framework with a central management focal point is the underlying cause of many situations in which the controls that have been designed and put into operation are less than fully effective.

The Bureau of Information Services has taken, or is planning to take, corrective action in response to most of the recommendations presented in this report. However, bureau management has noted that limited resources and other security priorities will make it difficult to establish target dates for the implementation of recommendations that are the responsibility of the newly created Risk Management Group.

Detailed findings along with recommendations for corrective action are presented in the following sections of this report. The full text of management's response is presented in Appendix III to this report.

ACCESS CONTROLS ARE INADEQUATE

Weaknesses in the RRB's system of password management undermine the effectiveness of access controls.

OMB Circular A-130 requires Federal agencies to implement and maintain a program to ensure that adequate security is provided for all agency information collected, processed, transmitted, stored or disseminated in general support systems and major applications. The circular further provides that agencies ensure that each system appropriately uses effective security products and techniques, such as password protection.

The RRB has not implemented an enforceable, effective password management program for its LAN/WAN and mainframe systems. As a result, RRB information systems are vulnerable to unauthorized access and the confidentiality and integrity of sensitive personal information maintained in those systems may be compromised.

The present system of password management is inadequate because the agency is unable to police and enforce its recently adopted policy requiring the use of more complex password configurations. We also noted other password-related control weaknesses in both the LAN/WAN and mainframe computing environments, including:

- passwords that never expire;
- inactive, duplicate system accesses;
- current employees with duplicate system accounts;
- separated employees whose system privileges had not been revoked; and
- accounts with which an employee-user could not be readily identified.

In addition, we identified the logon name and unencrypted password belonging to the system administrator of a major mainframe application by viewing a table in that application.

The agency's vulnerability to unauthorized access was confirmed by Blackbird Technologies, Inc., technical specialists under contract to the OIG. Using commercially available software, the contractor was able to break nearly one-third of LAN/WAN user passwords within six minutes.

The RRB is in the process of implementing prior recommendations for improved password management. The OIG will continue to monitor the implementation status of prior recommendations as part of the on-going audit follow-up process. We will assess the effectiveness of the agency's completed corrective actions during future reviews and make further recommendations as necessary.

LACK OF TRAINING UNDERMINES SECURITY PROGRAM MANAGEMENT

Employees with decision-making responsibility for information system security have not had adequate formal training in its theory, principles and practice. As a result, some employees do not have an adequate knowledge base to support the security-related decisions required by their positions.

Effective management of an organization's workforce includes training. Management should ensure that skills are continually assessed and that training is aimed at developing skill-levels to meet changing organizational needs. OMB Circular A-130 provides that responsibility for ensuring adequate system security should be assigned to an individual trained in the technology used in the system and in providing security for such technology, including the management of security controls.

During our review of information system security at the RRB, employees with key responsibilities for both the general support systems and the major applications advised us that they had not had training in the theory and practice of system security. Many employees with whom we spoke had input or decision-making responsibility for the design and implementation of security procedures and/or security-related software features.

The deficiency in security-specific training exists because, although the RRB provides training in software and hardware to employees with technical responsibilities, course selection is typically based on employee requests and tends to be software-specific. It appears that neither the operating staff, nor higher levels of agency management, recognized the potential long-term adverse impact that a lack of security-specific training could have on the security program as a whole.

Many conditions cited for correction in this report were caused by a lack of adequate training. Management and staff cannot make good decisions without adequate knowledge and skills. The lack of training among key personnel has a wide-ranging impact on planning and execution of information security for both the general support systems and major applications. As a result, this weakness in the RRB's information system security program poses a significant risk to the confidentiality, integrity, and availability of the agency's information systems.

Recommendation

1. The Chief Information Officer should develop and implement a plan to provide security-specific training to agency employees who have decision-making responsibilities for information systems. The plan should provide for training in the theory and practice of information systems security as well as training in the implementation of the security features of specific applications.

Management's Response

Management concurs with the finding and recommendation.

LACK OF A CENTRAL MANAGEMENT FOCAL POINT WEAKENS SECURITY

The RRB does not have a strong, centralized information system security program.

The General Accounting Office (GAO) has stated that a strong framework with a central management focal point and ongoing processes to coordinate efforts to manage information security risks is a key part of an effective computer security program. We believe that the absence of such a framework and focal point at the RRB is the underlying cause for many of the conditions cited later in this report.

In June 2000, the National Security Agency recommended that the RRB establish a formal security program, supported by upper management, with a full-time security officer to serve as the focal point. They further recommended that the security office be staffed with full-time, technical personnel who not only have the responsibility, but also have the authority to enforce security.

In July 2001, the agency began the process of appointing a full-time security officer. As of December 31, 2001, RRB management was in the process of interviewing potential candidates.

Since the agency is in the process of implementing a prior recommendation in this area, we will make no further recommendations for corrective action at the present time. We will evaluate the effectiveness of changes to the RRB's management structure in future reviews and make additional recommendations as necessary.

SECURITY PROGRAM DOES NOT FULLY COMPLY WITH OMB REQUIREMENTS

The RRB's information security program does not fully comply with the requirements established in OMB Circular A-130.

OMB Circular A-130 establishes a minimum set of controls to be included in Federal automated information security programs. The RRB is not in full compliance with the provisions of OMB Circular A-130 because, although the RRB has implemented an information system security program, some required features of the program have not been maintained in the prescribed manner. Our review identified deficiencies in:

- Security Plans
- Independent Evaluation
- Security Awareness Training
- Incident Reporting
- Disaster Recovery and Contingency Planning

We believe this condition exists because of the adverse impact that the absence of a central focal point for the agency-wide security program and the lack of security specific training has had on program management.

As a result, the RRB is not in full compliance with the provisions of OMB Circular A-130. Controls intended to ensure the security of agency information systems may not be fully effective, placing the RRB at increased risk of loss, misuse or unauthorized access.

Security Plans Are Outdated

The RRB has identified two general support systems and seven major application systems for which formal security plans must be prepared pursuant to OMB Circular A-130. That circular requires that security plans be developed and maintained for all Federal computer systems that contain sensitive information.

OMB Circular A-130 requires security controls be reviewed at least every three years. In addition, the RRB's Administrative Circular IRM-7 calls for security plans to be updated every two years.

The RRB's security plans are outdated. The security plan for the general support mainframe system was last updated in 1998. The plans for the general support LAN/WAN networks and major applications were last revised in 1995.

During June 2001, the RRB began the process of reviewing and revising its security plans.

Independent Security Evaluations Are Not Performed

The RRB has not performed periodic, independent evaluations of systems security in accordance with OMB Circular A-130.

OMB Circular A-130 requires that, at least every three years, an independent review or audit of the security controls for each major application should be performed. The circular specifies that the review should be independent of the manager responsible for the application.

Although the RRB performs periodic reviews of system controls in conjunction with preparation of the agency's security plan and its management control review activity, these reviews are not independent because they are conducted by the owners/users of the systems.

Security Awareness Training Is Not Adequate

OMB Circular A-130 requires Federal agencies to establish a security awareness and training program for both agency and contractor personnel. The circular calls for both initial training and on-going training to ensure that system users understand and abide by applicable rules.

The RRB provides very limited training, typically in the form of a written notice, to first-time system users and does not provide refresher training beyond periodic written reminders. New system users receive an information booklet “Information Systems Security Awareness Training for the Railroad Retirement Board (G-15).” New users are also expected to sign RRB Form G-15a, “Employee Acknowledgment Statement for the Information Resources Security Program of the Railroad Retirement Board.”

However, we were unable to locate a signed Form G-15a for 93 employees of a sample of 98 agency employees.[4] Based on this result, we must conclude that the RRB cannot demonstrate that it has provided adequate training and notice of possible sanctions for misuse of agency information systems.

The present program is not adequate to support adverse actions against employees who may misuse or compromise agency information systems. The reliance on written notice alone may not support an agency claim that an employee knew his or her rights, responsibilities and potential penalties for misuse.

Incident Reporting Procedures Are Not Sufficient

OMB Circular A-130 calls for Federal agencies to establish incident response capability to ensure that they can provide help to users when a security incident occurs in the system and to share information concerning common vulnerabilities.

The RRB has not established comprehensive procedures for reporting information security incidents. Existing procedures are not sufficiently specific to ensure that all incidents will be documented and shared internally and/or externally as appropriate to the situation.

Disaster Recovery and Contingency Planning Is Incomplete

OMB Circular A-130 requires the RRB to develop, maintain and test disaster recovery and continuity of operations plans for its general support systems and major applications. The objective of these plans is to provide continuity of data processing support if normal operations are interrupted.

During our audit, we observed that the RRB’s disaster recovery plan is outdated and incomplete. The plan has not been updated since September 1999 and does not include recently developed systems in its critical applications report, nor does it provide for the special equipment needs of those systems.

In addition, disaster recovery tests have not consistently included LAN/WAN applications other than establishing connectivity and general administration. The RRB has not verified results for LAN/WAN applications since August 1999.

[4] The original sample size was 120 randomly selected employees. We suspended testing based on the low identification rate for the first 98 items tested.

Recommendations

The Chief Information Officer should:

2. ensure that the RRB's security plans are updated timely and that independent comment and advice is sought as appropriate;
3. ensure that periodic independent evaluations of system security for major applications are performed;
4. provide ongoing security awareness training to agency employees and contractors;
5. establish effective guidelines and procedures for identifying and reporting security incidents;
6. update the overall disaster recovery plan; and
7. include LAN/WAN applications in the disaster recovery testing process.

As previously discussed, the RRB is in the process of appointing a full-time security officer. Accordingly, we make no recommendation for organizational change.

Management's Response

Management concurs with recommendations #3, #4, #5, #6, and #7.

Management neither concurred with, nor rejected recommendation #2. They noted that recommendation #2 is similar to recommendations issued in connection with two earlier audits and they plan to request that these two prior recommendations be removed from the OIG's audit follow-up program based on the "completed GISRA reviews and our commitment to update the plans."

OIG's Comments on Management's Response

The OIG tracks the status of all recommendations with which management has agreed until they have been implemented. Accordingly, recommendation #2 will remain in the OIG's audit follow-up system until corrective action has been implemented or the recommendation has been formally rejected.

MAINFRAME ADMINISTRATION NEEDS IMPROVEMENT

Security administration of the mainframe general support system is not fully effective and needs improvement.

OMB Circular A-130 requires that Federal agencies implement and maintain a program to ensure that adequate security is provided for all agency information collected, processed, transmitted, stored or disseminated in general support systems.

As a result of weaknesses in the administration of mainframe security controls, the confidentiality, security and integrity of the data processing system is at-risk of unauthorized modification, loss and disclosure. Our review identified weaknesses related to the maintenance of user accounts, the granting of system privileges, as well as the use of security rules and logs that indicate existing controls are not fully effective. In addition, we noted the duties of the ACF2 system administrator, a position critical to mainframe security, have not been formalized.

This condition exists because of the adverse impact that the absence of a central focal point for the agency-wide security program and the lack of security specific training have had on program management.

Account Maintenance

The Bureau of Information Services could improve routine maintenance to ensure that the privileges of separated employees are terminated promptly, all passwords expire periodically, inactive accounts are removed, and all users can be identified.

During our review of mainframe system security, we identified:

- 9 user accounts for which the passwords would never expire (8 contractors, 1 RRB employee);
- 7 employees with inactive, duplicate system accesses;
- 2 separated employees with active accounts; and
- 1 individual that could not be readily identified.

Least Privilege

We identified weaknesses in the application of the principle of “least privilege” in the mainframe environment. As a result, individuals have received and retained access to system features that they did not require for the performance of their assigned duties.

- Our review identified 32 individuals, including one non-employee on temporary detail to the RRB, who had been granted powerful privileges that they may not have required. These individuals were able to create, rename and delete files and data within the Federal Financial System. These are powerful privileges that should be closely restricted.
- The Bureau of Information Services does not maintain documentation to support the granting of special, high-risk, system privileges within ACF2. In some cases, these privileges may be required for a limited time. However, current procedure does not call for documentation of the reason for granting the privileges, the timeframe during which they should be retained nor does it provide for monitoring to determine whether the need for these rights continues to exist.

- The agency does not have an up-to-date listing of current ADVANTIS users and does not evaluate the need for on-going access on a periodic basis. The ADVANTIS system is a communications link that provides RRB employees with access to external data systems.

Security Logs

The ACF2 administrator does not use mainframe security logs effectively to detect and prevent security incidents.

Security logs may disclose situations that require timely action to prevent further risk to the agency's information systems. If the logs are not reviewed promptly, security incidents may go undetected and unreported. The ACF2 system creates a security log for all entries into the mainframe environment. These logs are intended to document security related incidents such as failed attempts at unauthorized actions and the use of high-risk special privileges.

During our review, we were advised that the ACF2 systems administrator reviews security logs only to confirm suspected security incidents. The administrator finds the logs too voluminous to permit the routine periodic reviews that would make them an effective security tool.

In addition, the ACF2 security logs do not capture information about the use of the most powerful, high-risk access privileges (termed "Allocate") that permit holders to create, delete, or rename files.

Continuity of Operations

The Bureau of Information Services has not formalized the procedures for the job of the ACF2 administrator. The ACF2 system controls mainframe security for critical applications and the systems administrator is responsible for system implementation and control activities. In the event that the systems administrator is not available to train a successor, the quality of security of ACF2 applications could be adversely affected.

Outdated ACF2 Security Rules

The ACF2 system controls the activities of the various software products that operate in the mainframe environment. ACF2 defines the scope of activities for each user of the mainframe system. One type of security rule is the user profile. User profiles control the mainframe application accesses of individuals within the agency user community. Another type of security rule controls the definition of privileges that govern access to files and programs by technical staff. This type of rule may apply to individual users or groups of users.

The ACF2 system includes outdated security rules for obsolete systems and software as well as user groups. Outdated security rules clutter the security management environment and weaken the overall information security structure.

Recommendations

We recommend that the Bureau of Information Services:

8. develop controls to ensure that the access rights of separated employees, temporary workers and contractors are terminated timely;
9. develop controls to ensure that the principle of least privilege is applied on an ongoing basis;
10. implement security logs as an effective control by ensuring that all critical activities are subject to logging and that logs are reviewed at least weekly;
11. develop formal procedures for the ACF2 system administrator; and
12. implement a control to ensure that outdated security rules are deleted from ACF2 timely.

Management's Response

Management concurs with recommendations #9 and #11 and has agreed to take the recommended corrective action. Management has stated that recommendations #8, #10, and #12 have already been implemented and plans no further corrective action.

OIG's Comments on Management's Response

Recommendations #8, #10, and #12 will remain in the OIG's audit follow-up system until the Bureau of Information Services has submitted documentation supporting implementation.

LAN/WAN SECURITY ADMINISTRATION NEEDS IMPROVEMENT

Security administration for the LAN/WAN general support system needs improvement. The present system of procedures and controls does not appear adequate to prevent the loss, misuse or unauthorized access to, or modification of, data stored in the system.

OMB Circular A-130 requires agencies to implement and maintain a security program to ensure that adequate security is provided for all agency information collected, processed, transmitted, stored or disseminated in general support systems. The Circular emphasizes management controls affecting individual users of information technology and requires periodic independent reviews of security in both general support systems and major applications.

The present configuration of staffing, hardware and software has resulted in a system that cannot be independently reviewed by agency management or third parties. LAN/WAN administrators did not have the software support to extract detailed information about LAN/WAN user accounts and system privileges in an efficient manner. Absent sufficient staff to assist auditors or other third parties in extracting the required information via a time-consuming, on-line review, the LAN/WAN system is, for all practical purposes, not auditable.

As part of the audit, we requested detailed information concerning the system privileges of LAN/WAN users. LAN/WAN administrators were not able to supply all required information from the system to permit timely review. They appeared to be pressured for time and hampered in their efforts by a lack of training in software and information system security. For example, responsible staff were unable to provide auditors with a listing of system users until the auditors had researched and demonstrated the capability of current software to support the request.

Once obtained, we analyzed the listing of LAN/WAN accounts and selected 42 for review of the identifying information and account status. The selection of accounts for further review was non-random and biased towards accounts that appeared to be questionable. The detailed review of these accounts revealed that:

- 20 LAN/WAN users had been granted a second account;
- 11 accounts were assigned to former RRB employees, of which only four had been disabled;
- four accounts assigned to temporary workers had not been disabled when their assignment/detail ended;
- five accounts with which an employee-user could not be readily identified from the information contained in the system; and
- eight accounts for which the password will never expire.

A detailed description of the specific control weaknesses that we identified during this audit follows. These weaknesses appear to be the result of the adverse impact that the absence of a centralized security program and lack of training has had on program management.

Account Maintenance

Based on our review, it appears that existing controls are not adequate to ensure that all holders of user accounts can be identified and that changes in employment status are recognized timely. Former employees whose accounts had not been disabled included five individuals who had separated more than a year prior to our review.

Some of the accounts for which the passwords would never expire had been assigned to contractors and group-users. One of the accounts with a non-expiring password had been assigned to a former employee whose account had not been disabled and who had separated from the agency in March 2000.

Least Privilege

Least privilege is the practice of restricting a user's access (to data files, processing capability, or peripherals) or type of access (read, write, execute, delete) to the minimum necessary to perform his or her job. The principle of least privilege is one of the controls required by OMB Circular A-130 for all general support systems.

The LAN/WAN administration function does not include periodic internal review and re-authorization of access privileges to the various LAN/WAN applications. As a result, the agency cannot ensure that user accesses have been restricted to the minimum necessary to perform their job in accordance with the principle of "least privilege."

We did not attempt to quantify the effect that this control weakness has had on the population of system users because the existing configuration of hardware and software would not support an efficient review process. System administrators were unable to extract information about the privileges of individual account holders except through an administrator assisted screen-by-screen online review. This lack of software support will hamper management in implementing an effective control.

Security Logs

LAN/WAN security logs are not reviewed routinely by systems administrators. As a result, incidents that could have an impact on information security may not be detected and reported.

During the audit, we were advised that current staffing levels do not permit routine review of system logs that could disclose potential violations of LAN/WAN security. LAN/WAN systems administrators review security logs primarily to research or document events that have already come to their attention.

Workstation Connectivity

The RRB has not implemented policy, procedures, and internal controls to address security issues resulting from inter-connection of personal computer hard drives. As a result, information stored on the hard drives of personal computers connected via the agency LAN/WAN system may be vulnerable to unauthorized access, loss and misuse.

During the audit, OIG auditors were able to open files on the hard-drives of four non-OIG, agency workstations from remote locations. One of the OIG auditors had never been granted access privileges to the agency's LAN/WAN. None of the viewable workstations had been password protected.

We were advised that the four workstations in the agency LAN/WAN had been individually configured to permit file-sharing with other workstations. As a result of this configuration, other users of the agency LAN/WAN and all users of the OIG LAN/WAN, because of its trust relationship with the RRB's LAN/WAN, had access to every file installed on those workstations, including the operating system and application software.

Recommendations

We recommend that the Bureau of Information Services develop:

13. the facilities to support detailed third-party security evaluation of user accounts and privileges;

14. a training program to ensure that LAN/WAN administration staff has adequate knowledge and skills to implement an effective security program; and

controls to ensure that:

15. user accounts fully identify the account holder;
16. unnecessary duplicate user accounts are disabled or deleted;
17. the LAN/WAN privileges of separated employees are curtailed promptly;
18. the LAN/WAN privileges of temporary workers and contractors whose assignments have ended are terminated promptly;
19. non-expiring passwords are used only when necessary;
20. the principle of least privilege is applied to the LAN/WAN general support system on an ongoing basis; and
21. workstation connectivity is controlled in accordance with a management policy designed to minimize risk of loss or misuse.

Management's Response

Management concurs with recommendations #13, #14, and #21 and has agreed to take the recommended corrective action.

Although management concurs with recommendation #20, they believe that the current operating system will not support development of the recommended control. They will examine this recommendation when a new operating system has been implemented.

Management has stated that recommendations #15, #16, #17, and #18 have already been implemented and plans no further corrective action.

Management does not concur with recommendation #19 stating that they "already have a control procedure for non-expiring passwords. They are only used for non-user name specific or generic ids."

OIG'S Comments on Management's Response

Recommendations #15, #16, #17, #18 will remain in the OIG's audit follow-up system until the Bureau of Information Services has submitted documentation supporting implementation.

It is regrettable that management did not voice their position concerning recommendation #19 during the discussion period that preceded issue of the draft report for formal comments. As presented in our findings, we identified instances in which non-expiring passwords had not been restricted in accordance with management's stated policy. This recommendation will remain in the OIG's audit follow-up system pending further discussion with the Bureau of Information Services.

APPLICATION LEVEL SECURITY SHOULD BE IMPROVED

OIG tests of user mainframe access profiles indicate that existing controls are not fully effective and that the security-awareness of system administrators could be improved. As a result, agency information systems may not be adequately protected from misuse or loss.

As discussed previously, OIG auditors were unable to complete audit tests of LAN/WAN security. Accordingly, our detailed findings pertain only to mainframe applications. However, Blackbird Technologies, Inc., during their security assessment of the LAN/WAN system noted that several LAN/WAN database applications allow easy access to the raw table data, as well as to form templates and modules leaving the data vulnerable to loss or unauthorized change. They also noted that source code in related applications could be easily viewed.

OMB Circular A-130 requires that all Federal agencies implement and maintain a program to ensure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in major applications. The circular also requires periodic independent reviews of security in both general support and major application systems.

We believe the weaknesses in mainframe and LAN/WAN security exist because of the adverse impact that the absence of a centralized security program and the lack of security-specific training have had on program management.

Least Privilege

The RRB has implemented controls intended to ensure that users of all major applications have been awarded privileges that are necessary to perform their jobs in accordance with the principle of "least privilege." The principle of least privilege is one of the controls required by Circular A-130 for all general support systems.

The primary means of ensuring that system privileges are consistent with job requirements is periodic review and re-authorization of access rights. However, some applications are not subject to the review and re-authorization process. In addition, responsibility for this process is scattered throughout the agency. The responsibility for initiating the review and re-authorization process rests with the Bureau of Information Services for some applications and with the system owner for others.

During our audit, we observed inconsistencies in the timing, documentation and effectiveness of the review and re-authorization process. The review and re-authorization process:

- has been performed for Personnel/Payroll and Financial Management applications less than annually;

- has not been performed for the FAST, SECUTAB, WILBUR, SURGE, and ZIPCO;[5] and
- typically relies on exception reports rather than positive confirmation of continuing user needs.

In order to test the effectiveness of agency controls, we compared the user profiles of 120 randomly selected employees with their job titles to determine whether their mainframe system application privileges were consistent with their present duties.[6]

Our review determined that 102 of the 120 employees in the sample (85%) had been granted privileges that were consistent with the needs of their position based on consideration of their job title (60 employees) or examination of written authorizations supporting the privileges as granted (42 employees).

Based on our review of job titles and the supporting documentation, we concluded that 18 of the 120 employees in the sample (15%) had been granted privileges that appeared to be inconsistent with their current employment comprised of:

- 4 employees whose access privileges were inconsistent with the supporting written documentation;
- 2 employees for whom the supporting documentation pertained to a prior position; and
- 12 employees for whom no supporting documentation was in the file for review.

The 18 user profiles questioned by the audit indicate that the controls intended to ensure that the principle of least privilege has been implemented at the application level are not fully effective and should be improved.

System Administrators

Implementation of information security at the application level has been adversely impacted by the lack of security-specific training among systems administrators. In addition, the RRB's system of information controls does not include reviews of system administrator activities that could have disclosed control weaknesses and the related training deficiencies.

Systems administrators for major applications have discretion concerning the implementation of application security features. During our review, we identified the following conditions that might have been questioned during an independent review of systems administrator activity:

[5] FAST, SECUTAB WILBUR, SURGE AND ZIPCO are mainframe applications that support the agency's benefit payment operations.

[6] A scope limitation, described in our discussion of the LAN/WAN general support system, prevented us from performing a similar test for LAN/WAN applications.

- an unencrypted system password for a user account with system administrator privileges was viewable in FFS tables;
- employees who administer the security features of the RUCS and FAST systems were also required, as part of their duties, to enter transactions for processing;[7] and
- logs that capture changes to data stored in Federal Financial System and Program Accounts Receivable System tables are not created for all tables that permit direct data entry.

Recommendations

The Bureau of Information Services should:

22. include all systems in the review and re-authorization process and mandate the frequency of the process for each system;
23. require a written response for all users during the review and reauthorization process; and
24. implement independent reviews of the system administrator functions throughout the agency.

Management's Response

Management concurs with recommendations #22 and #24 and has agreed to take the recommended corrective action. Management has stated that recommendation #23 has already been implemented and plans no further corrective action.

OIG'S Comments on Management's Response

Recommendation #23 will remain in the OIG's audit follow-up system until the Bureau of Information Services has submitted documentation supporting implementation.

SYSTEMS DEVELOPMENT

Documentation for the systems development lifecycle has not been consistently maintained. Existing controls are not adequate to ensure that all documentation can be located and that it is adequate to its intended purpose. As a result, the Bureau of Information Services has not adequately documented their performance of some security-related tasks that are a part of the systems development life cycle.

[7] RUCS and FAST are mainframe applications that support the RRB's benefit payment operations.

OMB Circular A-130 mandates consideration of systems security throughout the systems development life cycle.

Testing and Approval of Programs

The RRB has procedures intended to ensure that only programs and program changes that have been tested and approved by users are placed into operation. The Bureau of Information Services documents testing and approval of new programs and program changes manually using RRB Form G-872, “Sign-Off Sheet.”

However, current documentation is incomplete because it does not fully identify the version of the program that was tested and approved. Since there may be multiple versions of a program before it is approved and placed into production, the lack of a specific audit trail increases the risk that:

- an unapproved program may be placed into production, or
- a conflict may arise over responsibility for a program that does not function satisfactorily after being placed into production.

In addition, for one of the nine systems development projects reviewed during the audit, Form G-872 could not be located for three of the 15 programs that had been placed into production.

Consideration of Security in Systems Development

Current agency procedure requires execution of RRB Form G-402 “Security Profile,” or a similar document, for each automated application in development. The purpose of this form is to evidence the consideration of information security during the development of a new system or program changes that affect applications, information or processes. We identified two projects (of the nine reviewed during the audit) for which RRB Form G-402 had not been completed. As a result, the consideration of security in the development of the application could not be verified.

Cost Estimating Process

Current procedure requires that the Bureau of Information Services document initial cost estimates for new systems development projects using RRB Form G-436b, “Cost Estimate for ADP Project Service.” For one of the nine systems development projects for which we reviewed required documentation, the original Form G-436b was not available for review.

Recommendations

The Bureau of Information Services should strengthen controls to ensure that all activities in the system development lifecycle are adequately documented by:

25. revising current procedure to require full identification of the version of the program that was tested and approved when the G-872 is executed; and
26. developing a control to ensure that forms G-402 and G-436b are executed timely and maintained for review.

Management's Response

Management concurs with recommendations #25 and #26.

KEY CARD ACCESS TO THE DATA CENTER

The key card access system that is used to restrict physical access to the RRB's data center is not fully effective. As a result, the agency's risk of loss is increased.

The principle of least privilege dictates that a user's access to data files, processing capability or peripherals be restricted to the minimum necessary to perform his or her job.

Existing controls were not effective in detecting the granting of unnecessary privileges. Although the Bureau of Information Services states that it has implemented an informal manual review procedure using printed listings from the keycard system, no review documentation was available for examination during our audit.

The RRB's data center is comprised of 10 separate locations containing mainframe and LAN/WAN hardware, data communications equipment and data storage facilities. Each location is secured using a key card system. Access cannot be obtained without a keycard; the keycard's coding determines which of the 10 locations may be accessed.

During our review of the access privileges of key card holders, we identified an individual who had access to eight data center locations which was seven more than the single area required to perform his job.

Recommendation

27. The Bureau of Information Services should develop a control to identify errors in the access profiles of key cardholders.

Management's Response

Management has stated that recommendation #27 has already been implemented and plans no further corrective action.

OIG'S Comments on Management's Response

Recommendation #27 will remain in the OIG's audit follow-up system until the Bureau of Information Services has submitted documentation supporting implementation.

AUTOMATED FOLDER CONTROL SYSTEMS IS NOT PASSWORD PROTECTED

The decision to permit unrestricted access to one of the agency's folder control systems is not documented. As a result, the RRB does not have adequate assurance that risk has been properly considered in the security provisions for this system.

The RRB uses mainframe applications to track the location of RRB claim folders. Claim folders contain the paper documentation relating to benefit payment activity. Until the recent implementation of imaging technology, every claim for benefits was documented on paper and filed in a claim folder.

The Automated Folder Control System (AFCS) maintains the folder location history for the retirement, survivor and disability programs. The Unemployment Folder Control System (UFCS) tracks the claim folders used in the Unemployment and Sickness programs.

The AFCS is not password protected for general use. Although access to critical administrative functions has been restricted, anyone with physical access to mainframe screens can order folders from the off-site storage facility or change folder location codes within headquarters. Since the system is not password protected for routine transactions, it does not capture the identity of users who enter transactions.

Decisions concerning security should be risk-based, documented and periodically subject to review. The AFCS was originally implemented nearly 20 years ago and the decision to permit unrestricted access to routine transactions appears to date from that time. The AFCS is administered jointly by the Bureau of Supply and Service and the Office of Programs. Both organizations have appointed a system administrator; neither is aware of the existence of a more recent evaluation.

The UFCS is password protected for all transactions.

Recommendation

28. The Chief Information Officer should initiate an evaluation of the security needs of the AFCS and UFCS.

Management's Response

Management concurs with the recommendation.

APPENDICES AVAILABLE UPON REQUEST.