Review of the Systems Development Life Cycle for End-User Computing
Report No. 03-10, September 8, 2003

INTRODUCTION

This report presents the results of the Office of Inspector General's (OIG) review of the systems development life cycle for end-user computing at the Railroad Retirement Board (RRB).

Background

The RRB administers comprehensive retirement/survivor and unemployment/sickness benefit programs for railroad workers and their families under the Railroad Retirement Act (RRA) and Railroad Unemployment Insurance Act (RUIA). These programs provide income protection to railroad workers and their families during old age and in the event of disability, death, temporary unemployment, or sickness. The RRB paid over $8.8 billion in benefits during fiscal year (FY) 2002.

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 and wide area networks. Software applications in the end-user computing environment are accessed through personal computers connected to the agency's local and wide area networks.

The systems development life cycle is an essential component of information technology governance and helps ensure that new applications are adequately controlled and address the needs of the RRB. The principle phases of the life cycle are:

- Project Definition,
- Requirements Definition,
- Design,
- Coding,
- Testing, and
- Implementation.

The General Accounting Office (GAO) has issued standards specific to information systems development which include the documentation of requirements, authorizations for undertaking projects, reviews and testing, and approvals before placing systems into operation. The Office of Management and Budget (OMB) has also instructed agencies to apply National Institute of Standards and Technology (NIST) guidelines to achieve adequate security over Federal computer systems.

The RRB has published internal procedures for the development of new applications, including Administrative Circular IRM-10, "End-User Computing: Network and

Microcomputer (PC) Management," dated September 3, 1998; Administrative Circular IRM-11, "Security for Automated Information," dated June 17, 1994; and the ADP Standards. These procedures provide guidance regarding each phase in the systems development life cycle and establish control requirements to support the confidentiality, integrity, and availability of the information processed in the applications under development.

In general, the RRB's user bureaus initiate the development of new applications by forwarding a request to the Bureau of Information Services (BIS). BIS' E-Government Services section and representatives from the user bureaus cooperate throughout all phases of the development process.

The RRB's Office of Programs coordinates services to applicants and beneficiaries of the RRA and RUIA programs, and more than half of agency employees are assigned to that organization. The Office of Programs, as the largest of the agency's component organizations, submits the greatest number of requests for new computer applications and maintains a staff of system analysts to work with BIS program developers throughout the systems development life cycle.

The RRB has established the development of a sound and integrated information technology architecture as a strategic element of its larger objective to use technology and automation to foster fundamental changes that improve the way the agency does business. This audit directly supports this agency objective and will contribute to the annual OIG security evaluation mandated by the E-Government Act of 2002 (Public Law 107-347), Title III, the Federal Information Security Management Act of 2002.

Objectives, Scope, And Methodology

The objectives of this review were to assess:

- the adequacy of the RRB's methodology for the development and maintenance of end-user computing applications; and
- the effectiveness of the RRB's efforts in incorporating security requirements into the systems development life cycle.

In order to accomplish our objectives, we:

- reviewed applicable laws, regulations, NIST guidance, and RRB procedures;
- interviewed agency personnel responsible for systems development; and
- tested a non-random sample of 17 systems development projects for compliance with applicable RRB policy and procedure, and external authoritative sources such as NIST.

We selected the sample from a universe of 72 end-user computing development projects, started or completed during FY 2002 and FY 2003, as identified by BIS and

Office of Programs-Policy and Systems. Because BIS could not provide a complete inventory of projects, the universe may not have been all-inclusive. The 17 sample items were selected judgmentally by eliminating service requests that appeared to be routine maintenance or of such limited scope that their execution would not be representative of the systems development life cycle. Sixteen of the 17 projects reviewed had been requested by the Office of Programs.

Our work was performed in accordance with generally accepted government auditing standards as applicable to the objectives. Fieldwork was conducted at RRB headquarters during October 2002 through June 2003.

RESULTS OF REVIEW

In general, our review disclosed that the RRB does not have an adequate methodology for the development and maintenance of end-user computing applications; and the agency's efforts to incorporate security requirements into the systems development life cycle have not been effective. Specifically, the lack of a comprehensive life cycle methodology for the end-user computing environment has manifested itself in the following weaknesses:

- the agency does not have an effective project management program;
- the consideration of security is not fully incorporated into the systems development life cycle;
- authorization of new systems prior to implementation has not been ensured; and
- the testing and problem resolution phase of the life cycle is not comprehensive, is too informal and is poorly documented.

Management has agreed to take corrective action in response to all of the OIG's findings. However, BIS disagreed with our recommendation for development of a formal certification and accreditation process stating that the issue of non-compliance with existing procedures should be addressed, and describing their planned actions.

The details of our findings and recommendations for corrective action follow. The full text of management's response is presented as an appendix to this report.

Project Management Needs Improvement

Internal control over systems development in the end-user computing environment has been undermined by the lack of an effective project management system and the absence of a quality assurance program.

Internal control comprises the plans, methods, and procedures used to meet missions, goals and objectives. Internal control, which is synonymous with management control, assists managers in achieving desired results through effective stewardship. The

RRB's basic requirements for project management, as set forth in IRM-10, include preparation of a work plan that includes cost and resource estimates. Additional authorizations and analyses may be required for major projects based on the cost and resource requirements developed during the planning phase of the project.

During this review, BIS was unable to respond to auditor requests for an inventory of its workload, the status of project development and the staff resources expended to date. Our detailed review of 17 end-user computing projects indicates that the systems development life cycle is marred by a lack of documentation for critical activities. Our review disclosed:

- Nine projects that were not supported by a general work plan detailing required tasks and staff resources;
- 12 projects that lacked cost estimates; and
- two projects for which reliable estimates of staff time invested were not available.

During our review, we identified a major project that had not been submitted to the Information Technology Steering Committee (ITSC) for approval even though the work had progressed beyond the stage at which one would have expected such approval to be obtained. File evidence indicates that the project was expected to exceed the 1,000 staff hour threshold that mandated ITSC approval; however, no formal estimate of staff resources had been developed.

We also noted that the rationale for merging two new, smaller projects into an existing major project was not adequately documented, and that the paper trail of accountability for project authorization is undermined by procedures that often result in conflicting documentation.

The systems development life cycle for the end-user computing environment is not supported by a fully implemented project management system, manual or automated, that identifies major process steps, triggers required actions, or records expenditures of staff time. In addition, BIS has not implemented a quality assurance program to identify non-conformances in the execution of existing procedural requirements. In April 2003, BIS published procedures for a limited quality assurance program. These procedures are not sufficiently comprehensive with respect to existing standards and the program as currently implemented does not include a back-end review of compliance with agency standards and procedures.

As a result of the lack of a comprehensive project management system and quality assurance program, the efficiency and effectiveness of the systems development life cycle has not been ensured.

Recommendations

We recommend that BIS:

1. procure and install a new project management system;
2. implement a means to track the number of projects, the status of each project and the staff hours invested for projects under development until a new project management system is operational;
3. assess the feasibility of implementing a more comprehensive quality assurance function;
4. implement the quality assurance program as presently designed including a back-end review for compliance; and
5. implement a control to ensure that requests for ITSC approval are submitted timely.

Management's Response

Management agrees and plans corrective action in response to each of the five recommendations. BIS reports having completed requirements and selection of a replacement project management tool; however, procurement is dependent on the availability of funding. In addition, they plan to implement controls to track project status and ensure that ITSC approvals are secured when required until a new project management system is operational.

BIS has agreed to study the scope and requirements of a more comprehensive quality assurance function and assess the appropriate level of staff and tools needed. They will then make appropriate recommendations and proceed accordingly.

BIS has advised that they are incorporating architecture and capital planning investment compliance controls into the systems development life cycle in a staggered manner. They are currently performing analysis on how they might implement additional reviews, including a post-implementation review.

Security Has Not Been Integrated Into the Systems Development Life Cycle

Existing procedures and controls are not adequate to ensure the consideration of security in systems developed for the end-user computing environment in accordance with existing agency requirements as set forth in IRM-11. In addition, the RRB has not implemented a risk-based approach to authorization. We attribute these weaknesses to the lack of a comprehensive certification and accreditation process. As a result, new systems exhibit a lack of applied audit trails, weak authentication methods and poor access controls.

Our sample included two systems that were implemented without adequate access restrictions. The developer of one system in our sample retained post-implementation

responsibility for some tasks that required him to access production data. Proper separation of duties mandates that system developers work only outside of the production environment.

We also identified a system that had been implemented using shared user identification and password. Responsible management advised that this practice is contrary to agency policy; however, we were unable to identify formal standards or procedures communicating such a restriction.

Non-Compliance with Existing Agency Procedure

Controls are not adequate to ensure compliance with existing agency procedure as set forth in IRM-11.

IRM-11 requires the organizational unit requesting the systems development project to complete Form G-402, "Security Profile for Automated Application," or its equivalent. Form G-402 documents who is responsible for the security of each automated application, the sensitivity levels of the information handled by the application, and the control techniques that have been implemented to protect the information.

The 17 projects reviewed during our audit included 13 projects that had progressed to a stage at which the consideration of system security should have been documented. Our review disclosed:

- ten projects that had been placed into operation for which Form G-402, or an equivalent document, had not been prepared;
- four of the ten projects had no documented consideration of system security; and
- security control weaknesses exist in four of the ten projects that had been implemented without execution of Form G-402, or an equivalent.

The OIG previously identified the inadequacy of control over the preparation of Form G-402 in connection with the development of mainframe computer systems and recommended that BIS develop a control to ensure the timely execution and maintenance of Form G-402.[1] Accordingly, no additional recommendation for corrective action is offered at this time.

Authorization Levels Are Not Commensurate With Risk

The RRB has not established an authorization policy that assigns responsibility for pre-implementation authorization of systems development projects based on risk.

[1] "Review of Information Security at the Railroad Retirement Board," OIG Audit Report # 02-04, February 5, 2002.

In a risk-based approach to the systems development life cycle, higher levels of management authorize implementation of those projects that pose the greatest risk. The assessment of risk is key to placing accountability for implementation at an appropriate level within the organization. Typically, the greatest risk is associated with major applications and the systems with which they interface or exchange data.

Current agency procedure does not assign any authorization responsibilities to management level employees. Typically, user analysts who have been involved in a project's development and testing authorize implementation of completed systems on behalf of that organization. Some of these authorizations were offered informally, signatures were not always captured, and some had been transmitted by electronic mail.

RRB Lacks a Certification and Accreditation Program

Current RRB procedures are not consistent with trends in systems development which call for implementation of a formal certification and accreditation program that places responsibility for the acceptance of system security risk with higher levels of management.[2]

Certification is the comprehensive evaluation of the management, operational and technical security controls in an information system. Accreditation is the formal declaration of a management official that a system has been approved to operate at an acceptable level of risk. Through the accreditation and certification process, responsible management formally acknowledges responsibility for both system security and future accountability for any adverse impacts resulting from breaches of security.

OMB has highlighted the importance of the certification and accreditation process by requiring Federal agencies and their Inspectors General to report on the number of systems that have been certified and accredited.

IRM-11 places responsibility for documenting the consideration of system security with system users and developers. However, the RRB has not formalized the consideration of system security in a comprehensive certification and accreditation process.

Recommendation

6. We recommend that BIS develop a formal certification and accreditation process.

Management's Response

Management disagrees with the recommendation for a "formal" certification and accreditation process. BIS responded that, rather than develop new or changed procedures, the issue of non-compliance with existing procedures should be addressed.

[2]NIST is currently circulating draft standards for Federal certification and accreditation programs that specify "a senior agency official" as the appropriate level of management (NIST SP 800-37).

They plan to monitor NIST's distribution of standards and guidelines related to the certification and accreditation process. As these standards and guidelines become final, they will review them and consider whether a formal certification and accreditation process is needed.

BIS acknowledges that security control weaknesses found in applications that have been implemented without documented security profiles indicate that security controls were not considered and additional management controls are needed. They plan to issue revised procedures and designate an information system security officer for each major application and general support system.

Authorization Prior to Implementation Has Not Been Ensured

Internal control is not adequate to ensure that all systems will be properly authorized prior to implementation.

Current RRB procedure requires user testing and acceptance prior to implementation of new systems and system modifications. Form G-872, "Sign-off Sheet," is used by an authorized reviewer to accept or reject a final project. Form G-905, "Request to Install Software onto Server," is used to document authorization for installation of software, the person responsible for the installation, and the date that installation took place.

The ten projects in our sample that had been placed into operation included one project that had been placed into production without user testing and acceptance, and for which Form G-905 authorizing the software installation had not been prepared. It also appears that the system developer installed the application software, contrary to agency procedure calling for adequate separation of duties.

We also observed that two projects had been placed into production prior to formal acceptance by the user organization, and an additional seven projects for which Form G-905 had not been prepared.

RRB personnel have not followed existing procedures regarding the testing, acceptance, and authorization of projects prior to implementation. Additionally, RRB personnel have not documented all end-user computing installations. In the absence of adequate controls to ensure compliance with agency requirements, unauthorized systems or systems that do not meet the user's needs may become operational.

Recommendations

We recommend that BIS:

7. implement a control to ensure all projects are tested, accepted and authorized by the user organization prior to installation; and
8. implement a control to ensure that the installation process is properly documented and executed only by authorized individuals.

Management's Response

Management agrees and plans to implement a control to ensure that applications have been tested, accepted and authorized by the user organization before BIS supervisors authorize installation of applications and that the installation process is properly documented and executed only by authorized individuals.

Testing and Problem Resolution Needs Improvement

Execution of the testing and problem resolution phase of systems development in the end-user computing environment is not comprehensive, too informal, and not adequately documented. As a result, flawed systems may be placed into production.

Current RRB procedures require pre-implementation testing of all systems. Users and developers are required to develop a testing plan that addresses predetermined conditions derived from the program specifications and requirements document. The expected test outcomes should be defined within the plan and compared to actual test results. System developers are required to correct problems identified during the testing phase. System users are required to test and formally accept the software prior to installation.

The RRB has no controls in place to ensure that:

- test plans are properly developed and executed;
- problems are identified and addressed; and
- documentation supporting the testing and problem resolution process is maintained for subsequent review.

Our sample of 17 system development projects included 10 that had been completed and placed into production and one project undergoing pre-implementation testing. RRB personnel had not maintained test documentation and/or test plans for seven of the 11 projects. The four test plans that had been developed and submitted for review did not meet established agency requirements because they were incomplete. We also observed that the resolution of problems identified during testing was not formally controlled for three projects, including one for which the BIS developer did not return the correction to the user for verification and acceptance prior to implementation.

Our review identified one system that incorrectly computes certain estimated timeframes that are provided to annuitants concerning benefit changes under the Railroad Retirement and Survivors' Improvement Act. Pre-implementation testing performed by the Office of Programs did not disclose the calculation error because many possible input conditions were not tested. In that same project, test documentation of screen layouts differs from the layouts that are currently in production, indicating that changes were made after testing or that test documentation was not maintained.

As a result of weaknesses in the testing and problem resolution process, the RRB is at increased risk of implementing systems that produce inaccurate results and that may not meet the user's needs. In addition, the lack of documentation deprives the agency of a starting point for the oversight of system security in a comprehensive certification and accreditation process.

Recommendations

We recommend that:

9. the Office of Programs implement a control to ensure user testing is fully documented, including complete test plans and results; and
10. BIS implement a control to ensure developer testing is fully documented, including complete test plans and results.

Management's Response

Management agrees. The Office of Programs plans to provide additional training to their analysts. BIS plans to address issues specific to developer testing during their ongoing process of modifying the current system development life cycle to allow for methodologies specific to e-government solutions.

UNITED STATES GOVERNMENT

MEMORANDUM

FORM G-115f (1-92)

RAILROAD RETIREMENT BOARD

September 5, 2003

TO : Henrietta B. Shaw
Assistant Inspector General, Audit

FROM : Kenneth J. Zoll
Chief Information Officer
Dorothy Isherwood
Director of Programs

SUBJECT : Response to audit recommendations in the review of the systems development life cycle for end-user computing

The attached document includes the responses of the Bureau of Information Services and the Office of Programs to the audit recommendations detailed in the "Review of the Systems Development Life Cycle for End-User Computing" dated August 15, 2003. Our responses include a statement of concurrence or non-concurrence for each of the recommendations as well as target dates denoting when we anticipate the completion of corrective action.

Nine of the ten recommendations were addressed by the Bureau of Information Services. Recommendation Number 9, referring to user testing, was addressed by the Office of Programs.

Attachment

cc: Chief of E-Government Services
Chief Enterprise Architect
Director of Policy and Systems
Chief Security Officer

Responses to recommendations by the Office of Inspector General concerning the Review of the Systems Development Life Cycle for End-User Computing dated August 15, 2003

Recommendation 1. Procure and install a new project management system.

Response: Agree

We have completed requirements and selection of a replacement project management tool. A request has been submitted to the ITSC for funding for tools and services. The request is pending subject to further review and availability of funds. We anticipate a decision by October 15, 2003, as to whether full or limited funds for a pilot capable of managing three simultaneous projects will be approved. If approved, the acquisition of the system will be subject to available funding. Once funding has been obtained, we procure and install the new project management system.

Recommendation 2. Implement a means to track the number of projects, the status of each project and the staff hours invested for projects under development until a new project management system is operational.

Response: Agree

We have established a "Service Request Report" in the E-Government Services shared network storage space. The report is updated as G-436a requests are received or completed. We have instituted controls to ensure that status and staff hours are reported to the section supervisors weekly. The supervisors monitor and update the report as the staff hours are received. This control will be fully implemented by October 1, 2003.

Recommendation 3. Assess the feasibility of implementing a more comprehensive quality assurance function.

Response: Agree

We will study the scope and requirements of a more comprehensive QA function and assess the appropriate level of staff and tools needed. We will then make appropriate recommendations and proceed accordingly. We anticipate the study to be completed and recommendations forwarded to approving bodies by June 2004.

Recommendation 4. Implement the quality assurance program as presently designed including a back-end review for compliance.

Response: Agree

The Architecture and Planning Group has been incorporating architecture and capital planning investment compliance controls into the System Development Life Cycle in a staggered manner. We have recently completed implementing initiation controls for compliance and are currently performing analysis on how we might implement additional reviews including a post implementation review. The process will require the completion, review and approval of procedures. Training will also be needed. We anticipate the institution of a back-end review for compliance by August 2004.

Responses to recommendations by the Office of Inspector General concerning the Review of the Systems Development Life Cycle for End-User Computing dated August 15, 2003

Recommendation 5. Implement a control to ensure that requests for ITSC approval are submitted timely.

Response: Agree

We agree with the recommendation. As stated in the response to recommendation 3, the E-Government Services supervisors monitor and update the Service Requests Report at least weekly. As part of the weekly review, the supervisors ensure that the developers are following the system development life cycle (SDLC) as defined by the ADP Standards, which includes returning the e the PDD, along with the G-436A and G-436B, to the user to obtain ITSC approval if the project estimate exceeds 1,000 hours or more. This control will be fully implemented by October 1, 2003.

Recommendation 6. We recommend that BIS develop a formal certification and accreditation process.

Response: Disagree

We disagree with the recommendation that a "formal" certification and accreditation process be developed. Rather than develop new or changed procedures, the issue of non-compliance with existing procedures should be addressed. Current procedures require that the Security Profile for Automated Application (G-402) be completed. Security control weaknesses found in applications that have been implemented without documented security profiles indicate that security controls were not considered and additional management controls are needed. Revised G-436a procedures are soon to be released. The procedures have been modified to ensure that the security profile (G-402) is completed for application development requests. To address the accountability issue, we have identified the need to designate an information system security officer (ISSO) for each major application and general support system. These individuals will carry out specified duties as outlined in the security handbook. Members of the security domain team are currently reviewing a draft of the security handbook.

Note: We acknowledge that the National Institute of Standards and Technology is developing standards and guidelines for the certification and accreditation process. However, because they are still under development with a projected schedule for completing all publications, both standards and guidance currently projected for August 2004; it would be premature to develop a new process that has not be finalized. We will continue to monitor the distribution of these publications. As these standards and guidelines become final we will review them and consider whether a formal certification and accreditation process is needed. We shall develop a plan to make any necessary revisions to system develop life cycle procedures to ensure that appropriate security controls are included according to the level of risk to the respective security objectives (confidentiality, integrity and availability) and categorization of the information and information system.

Responses to recommendations by the Office of Inspector General concerning the Review of the Systems Development Life Cycle for End-User Computing dated August 15, 2003
Recommendation 7. Implement a control to ensure all projects are tested, accepted and authorized by the user organization prior to installation. **Response:** Agree BIS supervisors are responsible for signing the G-905 requests for installation of applications. The supervisors will ensure that the applications have been tested, accepted, and authorized by the user organization before signing the G-905 request. This control will be fully implemented by October 1, 2003.
Recommendation 8. Implement a control to ensure that the installation process is properly documented and executed only by authorized individuals. **Response:** Agree See the response to recommendation 7. This control will be fully implemented by October 1, 2003.
Recommendation 9. The Office of Programs should implement a control to ensure user testing is fully documented, including complete test plans and results. **Response:** Agree Testing is an integral part of any system development work. Back in 1999, P&S partnered with BIS to emphasize the need for thorough testing in the Y2K project and conducted a series of classes to support this. Last year, P&S hired a consultant to reinforce the importance of testing, to provide information on developing test plans and to discuss testing techniques. The subject is also part of the curriculum for a current class being conducted for analysts who have joined P&S in the past year. P&S section chiefs have already issued a reminder to staff that they are expected to create test plans and thoroughly test systems before implementation. We will consider this recommendation to be fully implemented upon completion of the user analyst training mentioned above. The target date is September 30, 2004.
Recommendation 10. BIS should implement a control to ensure developer testing is fully documented, including complete test plans and results. **Response:** Yes Developer testing is not a totally independent function. New methodologies, specific to end-user computing further integrate developer and user testing. We are in the process of modifying the current system development life cycle to allow for methodologies specific to e-government solutions. Issues specific to developer testing will be addressed at that time. We anticipate the completion of changes to the SDLC, approvals and training to be completed by the end of FY05.