Review of the Railroad Retirement Board's PIN/Password System for On-Line Authentication
Report No. 03-09, September 8, 2003

INTRODUCTION

This report presents the results of the Office of Inspector General's (OIG) review of the Railroad Retirement Board's (RRB) decision to use the Personal Identification Number (PIN)/Password System to authenticate Internet transactions.

Background

The RRB's mission is to administer retirement/survivor and unemployment/sickness insurance benefit programs for railroad workers and their families. During fiscal year (FY) 2002, the RRB paid approximately $8.7 billion in railroad retirement and survivor benefits to about 684,000 beneficiaries. The RRB also paid unemployment and sickness insurance benefits of $105.8 million to some 41,000 claimants.

Expanding electronic government, termed E-Government, is one of the five key elements of the President's Management Agenda. Initiated in July 2001, this effort is designed to make better use of information technology investments to eliminate billions of dollars of wasteful Federal spending, reduce the government's paperwork burden on citizens, and improve government response time. One of the ways the Federal government plans to accomplish these goals is by integrating technology investments across agencies.

The Government Paperwork Elimination Act requires Federal agencies, by October 21, 2003, to give customers the option of electronically doing business with the agency and to accept electronic signatures, when practicable. This Act specifically provides that electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form.

In light of this legislation, the agency plans to provide services to the public via the Internet. One of the issues facing the agency is how to protect the integrity and confidentiality of electronic records and transactions. Different methods of verifying the identity of the individual making the transaction offer varying levels of assurance for integrity and confidentiality. Among these methods in ascending level of assurance are:

- shared secrets methods (e.g. passwords),
- digitized signatures or biometric identifiers such as fingerprints, retinal patterns and voice recognition, and
- cryptographic digital signatures also known as Public Key Infrastructure (PKI).

Any of these approaches may be appropriate for a given transaction depending on the balance between the benefits from the electronic process and the risks of harm.

In November 2002, the RRB implemented a PIN/Password system to authenticate users of the RRB's Internet services. The agency's Office of Programs is primarily responsible for maintaining the system. The system presently allows current and former railroad employees to conduct some business with the agency on-line.

The PIN/Password System is the gateway to access several completed or planned RRB Internet services.

- The Service and Compensation On-line component allows railroad employees and annuitants to view their railroad service and compensation records via the Internet.

- The Retirement Planner component, which should be available in the near future, will provide annuity estimates on-line with direct links to an individual's service and compensation records.

- The Internet Unemployment and Sickness Insurance system will enable railroad employees to file unemployment applications and claims, as well as sickness claims, on-line. The unemployment applications portion of the system should also be available in the near future.

- Finally, the system that will allow individuals to apply for retirement annuities via the Internet is in the early development stage.

The RRB's 2002-2005 Strategic Plan includes goals to provide excellent customer service and to use technology to improve the way the agency does business. The Internet services are part of the agency's efforts to accomplish these goals.

Objective, Scope and Methodology

The objective of this review was to assess the agency's decision process in choosing the PIN/Password system for authentication of individuals using the agency's Internet services. The scope of our review was primarily limited to evaluating the planning and analysis performed by the RRB during fiscal year 2000 through the November 2002 implementation of the system.

To accomplish our objective, we reviewed applicable laws, regulations, and procedures; Federal guidance and agency practices; and agency planning documents. We also interviewed responsible management and staff.

This audit was conducted in accordance with generally accepted government auditing standards as applicable to the objective. Fieldwork was conducted at the RRB headquarters in Chicago, Illinois from April 2003 through August 2003.

RESULTS OF REVIEW

Our review determined that the RRB's decision process was inadequate because the agency did not perform the necessary risk and cost benefit analysis before selecting an authentication method.

Nothing came to our attention during this review to indicate that the RRB's PIN/Password system would not be an effective authentication method for the RRB's Internet services. However, we did not perform the analysis necessary to determine if this system is the best authentication method based on costs and risks. It is RRB management's responsibility to perform the analysis and make this determination. Also, we did not test controls for the system during this review, and therefore, we have no assurance that these controls are working as intended and are effective. The OIG will perform an evaluation of controls once the RRB performs the required risk and cost analysis.

We also noted that the RRB placed the PIN/Password system into production without developing retention schedules for the Federal records obtained and/or produced by the system. As a result, the system administrators deleted some feedback messages submitted by users, even though the RRB had not requested the authority to destroy these records. Based on our audit, the system administrators have stopped deleting these records and have agreed to develop the necessary retention schedules. Accordingly, we make no recommendation in this area.

Detailed findings and recommendations are discussed below.

Insufficient Decision Process

The RRB did not adequately follow Federal guidance in its evaluation and selection of an authentication method for the agency's Internet services. The agency did not sufficiently document its consideration of risks and controls. Therefore, we have no evidence that the agency adequately performed the Federally recommended risk analysis necessary to support the agency's decision to use the PIN/Password system. The RRB also did not perform the recommended cost benefit analysis.

The only documentation prepared by the agency was a limited analysis of its proposed Internet services. In this analysis, the RRB created three levels of security for Internet transactions. The highest level uses PKI. The next level uses data encryption and PIN/Password, and the lowest level uses only data encryption. The RRB then placed each of the proposed Internet services into one of the three security levels.

The RRB's documented analysis is insufficient because the agency:

- Provided no documentation for its determination of the appropriate security level for each of the Internet services.

- Did not document the inherent risks or the controls mitigating the risks for any of the proposed services.

- Did not assess or document the strengths and weaknesses of a PIN/Password authentication system or other alternatives.

- Moved on-line Unemployment and Sickness applications and claims from the PKI level of security to the lower PIN/Password level without any documented reason.

- Reconsidered the use of PKI for benefit applications because of concerns about PKI costs, frequency of RRB transactions, and implementation delays in the federal PKI program, but provided no detailed data to support this argument.

The Office of Management and Budget (OMB) issued guidance to assist agencies in implementing the Government Paperwork Elimination Act. The OMB guidance recommends an assessment on the use and acceptance of electronic documents and transactions including an evaluation of the suitability of electronic signature alternatives for a particular application. The assessment should include both a risk analysis and a cost benefit analysis. In performing the risk analysis, agencies should consider the relationship of the parties to the transaction, the value of the transaction, the risk of intrusion, and the future need for accessible and persuasive information regarding the transaction. The risk analysis should use a combination of quantitative and qualitative methods. The agency should document the decision on which combination of technologies, practices, and management controls minimize risk while maximizing benefits.

In November 2000, the Department of Justice (DOJ) issued guidance entitled “Legal Considerations in Designing and Implementing Electronic Process: A Guide for Federal Agencies.” The guidance recommends that, when deciding whether to convert paper processes to electronic ones, agencies should conduct an analysis of the transaction or process to determine the level of protection needed and level of acceptable risk.

The DOJ guidance also comments on the appropriateness of total conversion to a paperless process. Agencies should consider whether some paper documents should continue to be used. The guidance advises that sometimes “retaining a paper document might be the best, most certain, and easiest to prove medium for establishing a legally significant transaction or event.” The Government Paperwork Elimination Act does not require the use of electronic processes if an agency concludes that such use is not practicable for a particular transaction.

The National Institute of Standards and Technology has also provided guidelines for Federal agencies planning Internet services that require electronic authentication. The guidelines suggest a risk analysis similar to that recommended by OMB and DOJ.

RRB management did not believe that a cost and risk analysis was necessary because they believed the agency was following the efforts of other agencies. Several Federal agencies are using a PIN/Password system for some Internet transactions, but the OIG did not identify any agencies that are using the PIN/Password system as an electronic signature for benefit applications. For example, the Social Security Administration (SSA) offers on-line benefit applications, but the application must be printed and signed. Furthermore, SSA has suspended the expansion of its PIN/Password system pending the completion of a more comprehensive E-Authentication strategy. The Department of Veterans Affairs also has an on-line application, but requires a printed and signed signature page.

RRB management also relied on an October 2001 legal opinion from the RRB's general counsel who advised that there are no legal objections to using the PIN/Password system as an alternative to a signature. However, the legal opinion does not excuse the agency from a risk and cost analysis. The opinion referred to the November 2000 DOJ document that recommended performing a cost-based risk analysis to assess using electronic methods instead of paper transactions.

Management also relied on discussions with the OIG during development of the PIN/Password system. The OIG reviewed and commented on portions of the system as part of the agency's process to obtain OMB's approval to obtain personal information through the PIN/Password system. However, we did not perform the analysis necessary to determine if PIN/Password is the best authentication method based on costs and risks.

Because the RRB did not adequately follow guidance in this area, the agency may not have chosen the most cost-effective, risk-appropriate authentication method for each underlying Internet service. Without the risk assessment, the agency has not fully demonstrated that the PIN/Password system provides a sufficient level of authentication to meet the agency's litigation and administrative needs. In addition, the agency is at increased risk of incurring unforeseen costs to manage and maintain the password databases because the costs have not been quantified and documented. Finally, the agency has not documented that the PIN/Password system will adequately protect the agency against unlawful disclosure of personal information.

Recommendations

The Office of Programs should:

- perform and document a risk and cost benefit analysis for each of the railroad employee and annuitant Internet services. The analyses should determine whether PIN/Password is the most appropriate authentication method or if

another system of authentication (electronic or paper) should be used (Recommendation #1).

- complete the risk and cost benefit analysis prior to implementing the on-line unemployment, sickness and retirement benefit applications (Recommendation #2).

The Bureau of Information Services should establish procedures that comply with Federal guidance on selecting and implementing authentication methods for on-line services (Recommendation #3).

Management's Response

The Office of Programs concurs with recommendation #1. They advised that they have completed the analysis for the proposed unemployment and sickness services and will complete the analysis for the currently operational Internet services by March 30, 2004. The Office of Programs also concurs with recommendation #2. They will not implement any Internet benefit applications until after completion of the suggested analyses. A complete copy of their response, without attachments, is included in Attachment 1.

The Bureau of Information Services concurs with recommendation #3 and will update the appropriate Information Technology Standards and Procedures by the end of fiscal year 2005. A complete copy of their response is included in Attachment 2.

Recent OMB Mandate on E-Authentication Interagency Compatibility

On July 3, 2003, OMB issued a memorandum to all Federal agency Chief Information Officers stating that agencies should pursue a cross-agency approach for authentication and identity management. OMB advised that it is executing Federal-wide acquisitions of authentication technology, including PIN/Password, and is requesting agencies not to acquire authentication technology without prior consultation with the government-wide E-Authentication team.

OMB also advised that it is consolidating agency investments in credentials and PKI services. It will select shared service providers by December 31, 2003, with agency migrations to those selected shared service providers occurring throughout FY 2004 and 2005. In the memorandum, OMB advises: "There will be no new funding in FY06 for authentication or identity management investments not related to the selected shared service providers… Agencies should develop migrations plans to the shared service with planning work beginning now and a final plan expected following the selection of the shared service providers."

RRB management has been monitoring the E-authentication initiative and has agreed to consider this mandate in the analyses required in recommendation #1. The OIG will monitor compliance with this mandate to ensure that compatibility and the potential funding risks of non-compatibility are adequately reflected in the cost and risk analyses.

UNITED STATES GOVERNMENT

MEMORANDUM

FORM G-115f (I-92)
RAILROAD RETIREMENT BOARD

SEP 05 2003

TO: Henrietta Shaw
Assistant Inspector General, Audit

FROM: Catherine A. Leyser
Director of Assessment and Training

THROUGH: Dorothy Isherwood
Director of Programs

SUBJECT: Draft Report – Review of the RRB's PIN/Password System for On-Line Authorization

Response to Draft Report – PIN/Password System

Recommendation 1

The Office of Programs should perform and document a risk and cost benefit analysis for each of the railroad employee and annuitant Internet services. The analyses should determine whether PIN/Password is the most appropriate authentication method or if another system of authentication (electronic or paper) should be used (Recommendation #1).

OP Response

We agree and have completed such an analysis for the RUIA NET system (copy attached). We expect to complete the analyses for the Internet applications currently operational by March 30, 2004.

Recommendation 2

The Office of Programs should complete the risk and cost benefit analysis prior to implementing the on-line unemployment, sickness and retirement benefit applications (Recommendation #2).

OP Response

We concur. No such systems will be implemented until the suggested analyses are completed.

---

cc: Chief Information Officer
Director of Policy and Systems
Chief, Program Evaluation, Ret/Surv/Tax/Medicare

UNITED STATES GOVERNMENT

MEMORANDUM

FORM G-1151 (1-92)

RAILROAD RETIREMENT BOARD

September 4, 2003

TO : Henrietta B. Shaw
Assistant Inspector General, Audit

FROM : Kenneth J. Zoll
Chief Information Officer

SUBJECT : Draft Report – Review of the RRB's PIN/Password System for On-Line Authentication

We have reviewed the subject draft report dated August 21, 2003. Only one of the recommendations was directed to the Bureau of Information Services:

> Recommendation #3 – The Bureau of Information Services should establish procedures that comply with Federal guidance on selecting and implementing authentication methods for on-line services.

We agree with this recommendation. We are currently working to update and revise the IT Standards and Procedures which govern the Systems Development Life Cycle (SDLC). We will develop procedures to implement the recommendation as part of this project. We expect to complete this project in fiscal year 2005.

Your report also cites recent OMB instructions regarding the E-Authentication initiative. My staff continues to monitor this initiative and will include any OMB guidance in the SDLC standards and procedures as they are developed.

cc: Director of Programs
Chief Enterprise Architect
Chief of E-Government Services