Evaluation of the Self-Assessment Process
For Information System Security
Report No. 03-02, December 27, 2002

INTRODUCTION

This report presents the results of the Office of Inspector General's (OIG) evaluation of the self-assessment process for information system security 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.

The RRB's major application systems correspond to its critical operational activities: payment of RRA and RUIA 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.

An information security self-assessment is a key part of the annual agency program review process. The self-assessment process is used to determine the current status of a security program, and where necessary, to establish a target for improvement.

The Office of Management and Budget (OMB) has instructed agencies to apply National Institute of Standards and Technology (NIST) guidelines to achieve adequate security over Federal computer systems. NIST has published a self-assessment guide that presents a standardized approach for assessing system security using long-standing requirements found in statute, policy, and other guidance.[1] The guide establishes a minimum standard for evaluating the security of Federal information systems. It includes an extensive questionnaire containing specific control objectives, elements, and techniques against which systems can be tested and measured.

[1] NIST Special Publication 800-26, "Security Self-Assessment Guide for Information Technology Systems," November 2001.

The Government Information Security Reform Act (GISRA), signed into law October 30, 2000, required annual agency program reviews and annual Inspector General security evaluations, with subsequent reports to OMB and Congress. In FY 2001, agencies had wide latitude in selecting a self-assessment methodology. In FY 2002, OMB mandated implementation of the NIST methodology. Compliance with this requirement could be achieved through the use of the NIST self-assessment guide or an equivalent evaluation tool.

In FY 2002, OMB directed Federal agencies to confirm, as part of the GISRA reporting process, whether their assessment methodology was comprehensive with respect to key NIST standards. Although the RRB reported that their self-assessment process had sufficiently addressed all NIST objectives, the OIG disagreed. In its report to OMB, the OIG stated that "our evaluation of the RRB questionnaire confirms seven of the 17 NIST elements were addressed. However, the RRB questionnaire deals primarily with general policy and procedure issues and lacks sufficient coverage to match the specific control objectives and techniques provided by NIST."

Responsibility for the RRB's agency-wide information security program is vested in its Chief Information Officer. The Chief Information Officer, through his staff in the Bureau of Information Services, oversees planning, implementation and evaluation of information security including the self-assessment process. The RRB engaged the services of contractors to facilitate the agency's security self-assessments in FY 2001 and FY 2002.

The RRB has established the development of a sound and integrated information technology architecture, which includes information security, 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 objective.

OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of this review was to evaluate the effectiveness of the self-assessment process for information system security at the RRB during FY 2001 and FY 2002. In order to accomplish our objective, we:

- reviewed applicable laws, regulations, and NIST guidance;
- obtained and reviewed self-assessment questionnaires and responses;
- assessed agency compliance with OMB requirements and self-assessment guidance; and
- interviewed agency personnel responsible for the self-assessments.

Our work was performed in accordance with generally accepted government auditing standards as applicable to the objective. Field work was conducted at RRB headquarters during September and October 2002.

RESULTS OF REVIEW

The RRB's self-assessment process for information system security has not been effective in assessing the current status of the RRB's security program as a basis for future improvement. In general, we observed a lack of quality control for this contractor conducted process. Our review disclosed that the agency's FY 2002 self-assessment process was weakened by:

- inadequate coverage of NIST objectives, elements and techniques;
- anonymous, incomplete responses to the questionnaire that served as its basic evaluation tool; and
- a lack of supporting documentation.

In addition, the agency was unable to locate any significant amount of detailed documentation to support their contractor's conclusions for FY 2001.

Management concurs with our recommendations and has planned corrective action to improve the self-assessment process. The details of our findings and recommendations follow. The full text of management's response is included as an appendix to this report.

THE FY 2002 ASSESSMENT PROCESS WAS NOT NIST COMPLIANT

The RRB's FY 2002 security self-assessment did not adequately address control objectives, elements, and techniques established by NIST for Federal agencies.

OMB Circular A-130 instructs Federal agencies to apply NIST guidelines in order to achieve adequate security over their computer systems. NIST has developed a self-assessment tool that consists of an extensive questionnaire containing specific control objectives, elements, and techniques against which a system can be tested and measured.

During FY 2001, specialists under contract to the agency performed security self-assessments using the NIST questionnaire. The contractor assessed the status of security in four of the agency's nine major information systems.

In fiscal year 2002, the agency employed the services of a different contractor to facilitate its security self-assessment. That contractor evaluated all nine systems using a questionnaire developed by the International Organization for Standardization (ISO).

The ISO questionnaire did not fully address all NIST objectives, elements and techniques. A comparison of the ISO and NIST questionnaires showed that the subject matter was not comparable. For example, the NIST questionnaire addresses the control objective for personnel security related to an organization's employees; the ISO questionnaire focuses on security issues related to contractor personnel.

The RRB's contractor supplemented the ISO questionnaire with existing draft versions of computer security plans and follow-up interviews with agency personnel. However, since computer security plans do not contain an appropriate level of detail and the follow-up interview process was not fully documented, they are a poor substitute for a properly developed questionnaire. In addition, the change in methodology from FY 2001 to FY 2002 adversely impacts the comparability of the data gathered.

Agency personnel have indicated that time constraints influenced their decision to accept the contractor's methodology in lieu of the NIST questionnaire in FY 2002.

As a result, the self-assessment process does not provide a basis for determining whether the current status of information security represents an improvement or degradation in the quality of performance over the prior period. Absent a consistent, compliant process, the RRB will be forced to continually reapply its efforts in determining the initial status of security controls. This inefficient process restricts management's ability to build a valid plan of action for improvement.

Recommendation

The Bureau of Information Services should ensure that, whether performed by agency personnel or specialists under contract to the agency, the self-assessment process:

1. is comprehensive with respect to NIST objectives, elements, and techniques; and
2. provides a consistent basis for assessing changes in the agency's security status from year to year.

Management's Response

Management concurs with the recommendations and plans to implement an automated software tool developed by NIST to conduct future assessments. They also plan to incorporate the self-assessment process into existing procedures.

SELF-ASSESSMENT PROCESS IS INCOMPLETE

The FY 2002 self-assessment process was incomplete. Some questionnaires were not returned, responses to some questions were not credible, and the responding officials were not identified.

The General Accounting Office (GAO) Standards for Internal Control in the Federal Government state that information shall be recorded and communicated to management and others within the entity who need it, in a form and within a time frame that enables them to carry out their internal control and other responsibilities.[2] For an entity to run and control its operations, it must have relevant, reliable, and timely communications.

Questionnaires for each of the RRB's nine major systems were released to the responsible agency officials. However, responses were returned for only four systems. None of the responses were signed or dated so it is not possible to hold individuals accountable for the quality of their response. In addition, the questionnaires for the mainframe and end-user computing environments, which are the responsibility of the Bureau of Information Services, were incomplete and lacked credibility. One of the respondents had answered only half of the questions and both respondents denied knowledge of an agency security policy.

The RRB has no control in place to ensure that self-assessment questionnaires are completed, returned, and contain credible information. As a result, the agency has not collected the relevant, reliable, and timely information needed to complete the security evaluations.

Recommendation

3. The Bureau of Information Services should develop controls to ensure that the self-assessment process is complete and credible.

Management's Response

Management concurs with the recommendation. Management plans to implement an automated software tool to facilitate the self-assessment process that will permit the Bureau of Information Services' Risk Management Group to conduct an independent assessment and verification of the submitted results.

SELF-ASSESSMENT PROCESS IS NOT FULLY DOCUMENTED

The self-assessment process was inadequately documented in both FY 2001 and FY 2002. The self-assessment process is a significant internal control activity that should be fully documented. The RRB does not have controls in place to ensure that documentation to support contractor conclusions is retained in agency files. As a result, the basis for contractor conclusions about information security cannot be determined.

GAO Standards for Internal Control in the Federal Government state that internal control and other significant events need to be clearly documented, and that the documentation should be readily available for examination. The standards further state

[2] GAO/AIMD-00-21.3.1, November 1999.

that control activities need to be established to monitor performance measures and indicators. These control activities should validate the propriety and integrity of performance measures, and could call for assessments and analyses that lead to further action. In FY 2002, OMB established agency self-assessments as a key performance measure to be reported under GISRA.

Agency management was unable to locate completed questionnaires or other documentation to support the FY 2001 self-assessment. The FY 2002 self-assessment process included interviews with responsible management and staff to supplement the questionnaires that served as the basic assessment tool. Neither the questions used, nor the information obtained during the interviews, were fully documented. Only the general subject matter of interviews conducted in FY 2002 was recorded.

Future improvement in the RRB's security program will be dependent upon the agency's ability to assess relevant and reliable security information, and to plan further action accordingly. These plans of action may require periodic modification, which can only be efficiently accomplished through the review of reliably maintained documentation.

Recommendation

4. The Bureau of Information Services should ensure that the information gathered during the RRB's self-assessment process, whether performed by agency staff or specialists under contract to the agency, is clearly documented and maintained.

Management's Response

Management concurs with the recommendation. Management plans to implement an automated software tool to facilitate the self-assessment process that will provide the necessary means to obtain documented results for each self-assessment.

UNITED STATES GOVERNMENT

MEMORANDUM

FORM G-115f (1-92)

RAILROAD RETIREMENT BOARD

December 19, 2002

TO : Henrietta Shaw
Assistant Inspector General, Audit

FROM : Kenneth J. Zoll
Chief Information Officer

SUBJECT: Draft Audit Report – Evaluation of the Self-Assessment Process for Information System Security

We have completed our review of the subject report and submit to you our response regarding the recommendations.

Recommendations 1 and 2

The Bureau of Information Services should ensure that, whether performed by agency personnel or specialists under contract to the agency, the self-assessment process:

1. Is comprehensive with respect to NIST objectives, elements, and techniques; and
2. Provides a consistent basis for assessing changes in the agency's security status from year-to-year.

BIS Response for Recommendation 1: We concur with the recommendation that BIS shall ensure that the self-assessment process is comprehensive with respect to NIST objectives, elements and techniques. In order to comply with this recommendation the agency will begin using the automated software tool developed by NIST, called "ASSET" to conduct all future assessments of the major applications and general support systems. Additionally, we will incorporate the self-assessment process into existing procedures described in Administrative Circular IRM-7 *Security Plans for Information Technology Systems* and where applicable in IRM-11 *Security for Automated Information.* Target date to complete implementation of this recommendation is October 2003.

BIS Response for Recommendation 2: We concur with the recommendation that a consistent process be used from year-to-year in order adequate access the agency's security status. Target date to complete implementation of this recommendation is December 2004 when two consistent assessment will have been performed.

Recommendation 3

The Bureau of Information Services should develop controls to ensure that the self-assessment process is complete and credible.

BIS Response: We concur with the recommendation that BIS develop controls to ensure that the self-assessment process is complete and credible. In addition to implementing the use of the software tool "ASSET", the Risk Management Group (RMG) will use the "manager" component of the software to gather all system assessments and conduct an independent assessment and verification of the submitted results. Target date to complete implementation of this recommendation is October 2003.

Recommendation 4

The Bureau of Information Services should ensure that the information gathered during the agency self-assessment process, whether performed by agency staff or specialists under contract to the agency, is clearly documented and maintained.

BIS Response: We concur with the recommendation that BIS will ensure that the information gathered during self-assessment process is documented and maintained. Implementation and use of the automated software tool "ASSET" will provide the necessary means to obtain documented results of each self-assessment conducted beginning with the initial use in calendar year 2003 and any subsequent updates, thus providing maintenance of current state assessment of all major applications and general support systems. Target date to complete implementation of this recommendation is December 2004.