Review of Incident Handling and Reporting at the Railroad Retirement Board
Report No. 06-09, August 24, 2006

INTRODUCTION

This report presents the results of the Office of Inspector General's (OIG) review of computer incident handling and reporting at the Railroad Retirement Board (RRB). A computer incident is a violation, or imminent threat of violation, of computer security policies, acceptable use policies, or standard computer security practices.

Background

The RRB administers the retirement/survivor and unemployment/sickness insurance benefit programs for railroad workers and their families under the Railroad Retirement and Railroad Unemployment Insurance Acts. These programs provide income protection during old age and in the event of disability, death, temporary unemployment or sickness. The RRB paid over $9.2 billion in benefits during fiscal year (FY) 2005.

The RRB's information system environment consists of two general support systems: the mainframe computer, and the end-user computing system which supports the RRB's local and wide-area networks including the computer security incident capability program. The RRB has experienced relatively few computer incidents that successfully penetrated agency defenses during FYs 2005 and 2006 with usually no more than 30 isolated incidents in any one month. During that period, only one major incident had widespread impact within the agency.

This review was conducted pursuant to the E-Government Act of 2002 (P.L. 107-347), Title III, the Federal Information Security Management Act of 2002 (FISMA). FISMA mandates that the National Institute of Standards and Technology (NIST) develop standards and guidance, including minimum requirements, for the security of agency information and information systems. FISMA also established a Federal information security incident center, headed by the Department of Homeland Security's Computer Emergency Readiness Team (US-CERT), to compile and analyze security incidents and provide assistance to Federal agencies on current or potential information security threats and vulnerabilities. US-CERT has issued an official taxonomy which defines the incident and event categories and reporting timeframes for Federal agency reporting. The US-CERT Taxonomy is included as Appendix I to this report.

FISMA mandates that agencies develop, document, and implement an agency-wide information security program that includes procedures for detecting, reporting, and responding to security incidents. Additionally, FISMA requires the OIG to conduct an annual evaluation of the information security, including incident handling and reporting.

The RRB has developed policies and procedures to protect the information system environment, including communication networks and data, from unauthorized use, misuse, or abuse by both internal and external threats. The RRB Computer Security Incident Response Plan (CSIRP) procedures include incident handling and reporting

and the establishment of a Computer Emergency Response Team (CERT) comprised of Bureau of Information Services (BIS) employees. Each RRB CERT member has been assigned various roles and responsibilities for incident handling and reporting. A synopsis of each member's roles and responsibilities is presented in Appendix II.

The RRB CERT manages computer security incidents as they occur. Computer security incidents can be identified in a number of ways. If a user detects unusual activity, he will report it to the Help Desk. Additionally, RRB CERT members are responsible for reviewing agency logs for suspicious activity. The logs may be produced by the operating system, access control software, antivirus software, data communication devices, or the intrusion detection system. After the RRB CERT member confirms the existence of a computer security incident, they respond by containing and eradicating the threat, and restoring the system if necessary.

The RRB CERT member responding to the incident is required to maintain documentation that may consist of the logs identified above, or forensically sound and legally admissible evidence for more serious incidents. Additionally, the lead investigator maintains a separate RRB CERT log of incidents by assigning a unique case number and details about the incident. This log is used to compile incident reports internally for RRB management, and externally for the US-CERT.

The RRB CERT continually works to improve the RRB's computer security infrastructure. They have reported several initiatives which they believe will enhance the RRB's computer security incident capability. These initiatives include an intrusion prevention system, policy enforcement software, and new help desk and spam prevention software. Additionally, they reported the completion of a special project to ensure all desktops have been fully patched to allow for more efficient distribution of future desktop upgrades and virus definition files.

A glossary of technical terms is included at Appendix III.

Objective, Scope and Methodology

The objectives of this review were to:

1. Determine whether the RRB's incident handling and reporting program is operating effectively to ensure the confidentiality, integrity and availability of the RRB's information and information technology.

2. Determine whether the RRB's program meets the standards and guidelines established by the US-CERT for external reporting.

To accomplish these objectives, we:

- interviewed responsible management and staff;

- obtained and reviewed the RRB's policies and procedures for incident response and reporting;
- obtained evidence of the RRB's computer security incidents and actions taken during FYs 2005 and 2006, including, but not limited to, logs, correspondence, and internal and external reports;
- obtained and reviewed NIST criteria for incident handling and minimum control requirements;
- obtained and reviewed US-CERT criteria for incident reporting;
- obtained and reviewed US-CERT compilations of reports made by the RRB;
- performed comparative analysis of the RRB's policies and procedures to the criteria established by NIST and US-CERT;
- assessed the agency's overall compliance with the applicable standards and guidance for incident response handling and reporting by comparing the RRB's actual incidents and reports to the RRB, NIST and US-CERT criteria; and
- obtained and reviewed the RRB's Plan of Actions and Milestones for previously identified information security weaknesses.

The scope of our audit did not include program improvement initiatives reported by management which were not completed prior to the start of fieldwork.

Our work was performed in accordance with generally accepted government auditing standards as applicable to the objectives. Audit fieldwork was conducted at RRB headquarters in Chicago, Illinois from January through May 2006.

RESULTS OF REVIEW

The RRB's incident handling and reporting program is generally operating effectively in ensuring the confidentiality, integrity and availability of the agency's information and information technology. However, the agency's program does not fully comply with standards and guidelines established by the US-CERT for external reporting, and we observed areas in which the RRB's program should be improved to ensure that the agency's risk has been minimized. The following deficiencies will be classified as reportable conditions in our FY 2006 evaluation of information security.[1]

- The RRB's response plan is not always followed.
- Malware incident prevention and handling needs improvement.

[1] A reportable condition exists when a security or management control weakness does not rise to the level of a significant deficiency, yet is still important enough to be reported to internal management. A significant deficiency is a weakness in an agency's overall information system security program or management control structure, or within one or more information systems, that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets.

- External reporting does not fully comply with US-CERT Requirements.
- Internal reporting is incomplete.
- The current patch management process is not fully effective in minimizing risk from known vulnerabilities.

In addition, we observed that the RRB's formal plan of action and milestones for program remediation does not include previously identified weaknesses in the incident handling and reporting process.

Management has agreed to take the recommended corrective action. The full text of the Bureau of Information Services response is included in this report as Appendix IV.

Computer Security Incident Response Plan (CSIRP) Is Not Always Followed

The RRB CSIRP provides the methodology to be used by the RRB CERT; yet, RRB CERT members do not always follow CSIRP procedures. In some cases, RRB CERT members were unaware of, or did not understand, all of their roles and responsibilities listed in the CSIRP. Our review of the CSIRP and current practice showed discrepancies in the following areas.

- Some of the roles and responsibilities of the RRB CERT are not followed, including oversight of RRB CERT activities.
- Documentation supporting all RRB CERT members' actions is not completed by members outside of the BIS Risk Management Group, or consistently within the Risk Management Group.

FISMA requires agencies to develop "procedures for detecting, reporting, and responding to security incidents." NIST Special Publication (SP) 800-61 provides guidance on the development of policies and procedures for incident response capability.[2] That guidance states that the operating procedures are the technical processes, techniques, checklists, and forms used by the incident response team. NIST requires the procedures to be comprehensive and detailed enough to ensure the agency's priorities are reflected in the response operations. Additionally, the procedures should be tested and validated for accuracy and usefulness, and distributed to all team members. Training is also to be provided to the team members, and incident response documents can be used as an instructional tool for reinforcement.

The CSIRP was designed to represent best practices and the expected procedures of the RRB CERT. However, the RRB CERT members have been given wide latitude in the methodologies used to respond to and record incidents. The Chief Security Officer has operational authority over the RRB CERT, but provides little or no oversight of RRB CERT activities. We found that current practices of the RRB CERT members do not always conform to the procedures within the CSIRP. Additionally, previous management control reviews were insufficient to determine the effectiveness of the

[2] NIST SP 800-61, "Computer Security Incident Handling Guide," January 2004.

incident response program. While revisions to the management control process are currently underway, ongoing supervision and training is needed to ensure adherence to the operating procedures.

The RRB incident response capability is impaired when employees do not perform their expected roles and responsibilities. As a result, computer security incidents may not be handled as effectively as they could be.

Recommendations:

We recommend that the Bureau of Information Services:

1. conduct training of the RRB CERT members' roles and responsibilities; and

2. implement controls to ensure the continued adherence to, and usefulness of, the CSIRP procedures.

Management's Response

The Bureau of Information Services concurs with the recommendations and will conduct training of the RRB CERT members and implement controls to ensure continued adherence to the CSIRP procedures.

Malware Incident Prevention and Handling Needs Improvement

Our review disclosed several inefficiencies in the RRB's malware protection program, including inconsistent antivirus software configuration settings and missing or incomplete logs.

FISMA requires agencies to develop "procedures for detecting, reporting, and responding to security incidents … including mitigating risks associated with such incidents before substantial damage is done." NIST SP 800-83 provides guidance on malware incident prevention and handling.[3] That guidance states that malware prevention-related policy considerations should include "specifying which types of preventive software (e.g., antivirus software, spyware detection, and removal utilities) are required … and listing the high-level requirements for configuring and maintaining the software (e.g., software update frequency, system scan scope and frequency)."

RRB management has not established a formal antivirus software configuration policy which specifies the requirements for configuring and maintaining that software. Discussions with RRB CERT members revealed that their assumption of how the antivirus software is configured is inconsistent with the configurations displayed on the antivirus logs. The lack of a formal configuration policy, and procedures for documenting and approving deviations from that policy, can lead to ineffective practices.

[3] NIST SP 800-83, "Guide to Malware Incident Prevention and Handling," November 2005.

We also noted that the antivirus software's threat history logs were incomplete for two months, and the RRB has been unable to produce the logs since January 2006. An actual cause of the missing log entries is unverifiable; however, RRB management believes problems with the software resulted in the missing data. The RRB has been unable to produce the threat history logs for several months because they appointed a new antivirus administrator who requires specialized training in the use and management of the software. The RRB did not have a valid backup administrator with this knowledge.

Threat history logs represent a primary source of information on RRB computer security incidents. The inability to produce the threat history logs impacts the identification, handling, and reporting of computer security incidents.

Recommendations:

We recommend that the Bureau of Information Services:

3. develop a formal antivirus configuration policy;
4. implement procedures for adequately documenting and approving deviations from that policy;
5. appoint a backup administrator for managing the antivirus software; and
6. provide adequate training to the new antivirus administrator and backup administrator.

Management's Response

The Bureau of Information Services agrees with the recommendations. They will develop a formal configuration policy and implement procedures for documenting deviations from that policy. Additionally, the Bureau of Information Services will appoint a backup administrator and provide training to the two network administrators designated as Norton Anti Virus administrators.

External Reporting Does Not Fully Comply with US-CERT Requirements

The RRB's reporting of computer security incidents to US-CERT needs improvement. Our review disclosed that the RRB's incident reports did not conform to US-CERT reporting requirements, and were often incomplete. The most significant category of inadequate reporting was for successful malicious code identified by antivirus software.

FISMA requires agencies to notify and consult with the Federal information security incident center, US-CERT, regarding computer security incidents. The US-CERT has issued guidance which defines the reporting categories and timeframes to be used by Federal agencies.[4] This guidance is designed to ensure a consistent means of reporting and to provide a common platform to execute the US-CERT mission. US-

[4] The US-CERT Taxonomy is included as Appendix I.

CERT requires that successful malicious code that could not be quarantined by antivirus software be reported daily.

The RRB did not comply with the US-CERT reporting requirements because the lead investigator responsible for preparing the reports made a conscious decision to deviate from the guidance. He stated the criteria for daily reporting of isolated successful malicious code is unreasonable, and has decided not to follow it. Instead, he has chosen to report a compilation of these incidents on a monthly basis.

We also noted that the RRB's monthly compilation reports made to US-CERT did not include all instances of reportable security incidents. The lead investigator did not make RRB CERT log entries for all reportable incidents. Often, log entries are only made when he performs the CERT activity himself because he does not receive the information from other CERT members in a timely manner. For example, he is notified of isolated incidents involving malicious code identified by the antivirus software at the end of the month, rather than when the incident occurred. BIS management has not ensured an effective means of communicating and reporting successful malicious code between team members.

Nonconforming and incomplete external reports made to US-CERT restricts their ability to perform their mission. The Office of Management and Budget (OMB) has indicated in its FY 2005 Report to Congress that "Less than full reporting hampers the government's ability to know whether an incident is isolated at one agency or is part of a larger event, e.g., the widespread propagation of an Internet worm."[5]

Recommendations:

We recommend that the Bureau of Information Services:

7. implement controls to ensure incident reports released to US-CERT are complete, accurate, and conform to US-CERT requirements; and
8. implement a system to track and communicate all incidents, including successful malicious code identified by the antivirus software, from discovery to completion and final reporting.

Management's Response

The Bureau of Information Services generally concurs with the findings and has agreed to implement controls to ensure complete and accurate incident reports released to US-CERT. However, the Bureau of Information Services is not currently prepared to ensure those reports fully conform to US-CERT requirements. They have agreed to resolve the reporting issues associated with the antivirus software, and to provide for a link between the antivirus administrator and help desk ticketing software to provide timely and documented antivirus responses. When the link is established, the antivirus

[5] "FY 2005 Report to Congress on Implementation of The Federal Information Security Management Act of 2002," March 1, 2006.

administrator will be responsible for ensuring the reports are made in conformance to US-CERT requirements.

Internal Computer Security Incident Reporting Is Incomplete

Reporting of computer security incidents to RRB management needs improvement. Our review disclosed discrepancies between incident records and incident reports made internally to RRB management, as well as delays in the reporting process.

FISMA requires agencies to implement a computer security incident response program that includes incident reporting. The RRB CERT is responsible for issuing a formal report of major incidents to RRB management. Additionally, the RRB CERT reports the number of incidents in the monthly BIS Administrative Report. The current incident categories reported are:

- RRB CERT cases opened;
- phishing attempts;
- spam emails;
- successful malicious code; and
- intrusion detection system events on the public-facing web server.

We found that the monthly BIS Administrative Reports did not include all instances of malicious code. For example, our interviews with BIS staff disclosed that the most prevalent security incident experienced by the RRB is spyware. However, there is no separate category for reporting spyware, and spyware that has not been detected by the antivirus software is not included in the compilation of successful malicious code.

We also noted that RRB CERT log entries were not made, nor adequate documentation retained, for all spyware incidents. Of the eight CERT log entries made during the months of October through December 2005, five were for malicious code, four of which involved spyware. Only two of the four spyware cases have adequate supporting documentation. We also noted that log entries for other types of incidents contained inaccurate data when compared with CERT case documentation.

Additionally, our review of the three months of antivirus logs that were available in FY 2006 showed that the number of computers infected in October had been miscounted. The BIS Administrative Report over-reported the number of infected systems by four. Antivirus logs are made available to the RRB CERT member responsible for preparing the incident reports at the end of each month. Due to the volume of entries on the log (both successful and unsuccessful malicious code), errors in counts can easily be made.

The RRB's major incident in August 2005 required the preparation of a formal report for RRB management. However, as of March 2006, that report has not yet been issued. We were told that the RRB CERT made several recommendations to BIS management, and are awaiting a decision on those recommendations. They have chosen to wait until the decisions are made before issuing the final report to RRB management.

As previously noted, the Chief Security Officer has operational authority over the RRB CERT, but provides little or no oversight of RRB CERT activities. Inaccurate, incomplete, or delayed internal reporting prevents RRB management from adequately assessing the risk involved in RRB programs. Likewise, untimely reports lose their effectiveness in notifying higher levels of management of the status and issues involved.

Recommendations:

We recommend that the Bureau of Information Services:

9. implement controls to ensure internal reports of incidents are accurate and complete; and
10. issue reports of major incidents to RRB management as soon as the nature of the incident is known, rather than when recommendations for future actions are implemented.

Management's Response

The Bureau of Information Services concurs with the recommendations and will adopt controls specified in NIST SP-800-53. Additionally, the Bureau of Information Services agrees to revise their procedures to have final incident reports available to the CIO within 60 days of incident closure.

Current Patch Management Process Is Not Fully Effective In Minimizing Risk

RRB systems continue to be at risk for major security incidents. The OIG has reported numerous times, dating back to July 2001, that the RRB did not have security patches and updated service packs installed on their servers. RRB patch installations on network servers are generally performed manually over multiple weeks, with automated desktop patches installed thereafter.

NIST Federal Information Processing Standards Publication 200 establishes the NIST SP 800-53 as the "Minimum Security Requirements for Federal Information and Information Systems" effective March 9, 2006.[6] Federal agencies must be in compliance with these standards by March 9, 2007. NIST SP 800-53 requires Federal agencies to identify, report, and correct information system flaws by promptly installing newly released security relevant patches, service packs and hot fixes, and testing software for effectiveness and potential side effects on the agency's information systems before installation.

NIST SP 800-53 also requires agencies to develop, disseminate, and periodically review and update formal, documented system and information integrity policies and procedures that address the control area of which flaw remediation is included.

[6] NIST SP 800-53, "Recommended Security Controls for Federal Information Systems," February 2005.

The RRB management has not adopted formal patch management policy and procedures that ensure patches are installed quickly and effectively. Microsoft Corporation releases patches on the second Tuesday of each month, and gives customers advance notice on the Thursday before the patch is released. This notice includes the products that will be patched and the severity of the vulnerabilities associated with the patch. Recent trends show that hackers take advantage of newly disclosed software flaws which compel organizations to implement better processes for testing and installing patches quickly and effectively.

For example, in August 2005, the RRB experienced a major computer security incident with widespread agency impact. The Microsoft patch for that vulnerability was released on August 9, 2005. The RRB's infection occurred during the week of August 14, 2005. Agency antivirus logs indicate that the security incident which first occurred in August was still affecting the RRB's information systems the following November. Yet, other Federal agencies claim to have experienced little, if any, impact on their networks because they tested and implemented the patch from Microsoft in less than three days.

While patch installation is no guarantee that a security incident will not occur, a properly designed, effective patch management program should reduce the risks associated with identified vulnerabilities. Timeliness is a key part of an effective patch management program.

The BIS Network Services Group developed the procedures it currently follows after the August 2005 incident: an undocumented, informal, patch management process based on "increased awareness." However, over time, informal procedures can degrade due to resource constraints and complacency when the original emergency has passed.

The BIS Risk Management Group has drafted a patch management policy which delineates, on a priority basis, the devices and timing for patch management. This plan allows up to 30 days for completion of action on some patches, depending on the assigned priority. No decision has been made regarding whether to adopt this, or a more aggressive policy.

A faster, smoother method of installing patches throughout the RRB should be implemented, utilizing a checklist to ensure all affected systems are appropriately patched. Documentation of the patch installation should be maintained to support verification of patch completions.

Recommendation:

11. We recommend that the Bureau of Information Services develop and implement a formal policy and procedure addressing patch management.

Management's Response

The Bureau of Information Services has agreed to develop and implement a formal patch management policy and procedure.

Known Weaknesses Are Not Included in the RRB's Plan of Action and Milestones

The agency's Plan of Action and Milestones (POAM) does not include previously identified weaknesses in the RRB computer security incident response program.

FISMA requires Federal agencies to maintain a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security, policies, procedures, and practices of the agency. The OMB requires agencies to prepare an agency wide POAM incorporating all known information security weaknesses associated with information systems used or operated by the agency, a contractor of the agency, or any other organization on behalf of the agency. OMB also requires the agency to prepare quarterly updates of the progress in implementing remedial actions and identifying problems, and an OIG evaluation of the POAM process.

In our FY 2005 FISMA report, we stated that the RRB's POAM was not comprehensive with respect to identified weaknesses, and not driven by internal risk assessments and control evaluations. We also reported that the existing plan did not demonstrate prioritization of agency plans and efforts to correct information security weaknesses. We recommended that the agency improve its remedial action process to ensure all security weaknesses are included in the POAM and ensure that the plan demonstrates the prioritization of agency remediation efforts.[7]

During our FY 2005 FISMA review, we also identified weaknesses in the agency's procedures for incident response handling and reporting. These weaknesses were conveyed to RRB management through the OIG's OMB FISMA Template Report issued on October 5, 2005. As of May 31, 2006, the RRB had released two quarterly updates of its POAM, neither of which reflects the weakness we identified in the OMB FISMA Template Report. Prioritization of remedial actions and an adequate assessment of risk cannot be achieved without inclusion of all security weaknesses.

This finding will be considered when we evaluate the RRB's remedial action process as part of the OIG's FY 2006 FISMA evaluation and reporting process.

Agency action to implement prior OIG recommendations for corrective action is pending; the OIG has no additional recommendations to offer at this time.

[7] "Fiscal Year 2005 Evaluation of Information Security at the Railroad Retirement Board," OIG Report No. 05-11, September 28, 2005.

APPENDIX I

US-CERT Federal Agency Reporting Taxonomy
Federal Agency Incident Categories

CATEGORY	NAME	DESCRIPTION	REPORTING TIMEFRAME
CAT 0	Exercise/Network Defense Testing	This category is used during state, federal, national, international exercises and approved activity testing of internal/external network defenses or responses.	Not Applicable; this category is for each agency's internal use during exercises.
CAT 1	Unauthorized Access*	In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource.	Within one (1) hour of discovery/detection.
CAT 2	Denial of Service (DoS)*	An attack that *successfully* prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.	Within two (2) hours of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity.
CAT 3	Malicious Code*	*Successful* installation of malicious software (i.e., virus, worm, spyware, bots, Trojan horse, or other code-based malicious entity that infects or affects an operating system or application. Agencies are NOT required to report malicious logic that has been *successfully quarantined* by antivirus software.	Daily. Note: Within one (1) hour of discovery/detection *if* widespread across agency.
CAT 4	Improper Usage*	A person violates acceptable computing use policies.	Weekly

*Defined by NIST Special Publication 800-61

Federal Agency Event Categories

CATEGORY	NAME	DESCRIPTION	REPORTING TIMEFRAME
CAT 5	Scans/Probes/ Attempted Access	This category includes an activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.	Monthly. Note: If system is classified, report within one (1) hour of discovery.
CAT 6	Investigation	*Unconfirmed* incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.	Not Applicable; this category is for each agency's use to categorize a potential incident that is currently being investigated.

The US-CERT Taxonomy as published on the US-CERT website: www.us-cert.gov.

APPENDIX II

RRB CERT MEMBER'S ROLES AND RESPONSIBILITIES

Chief Information Officer (CIO)

The CIO is delegated operational responsibility for the protection of the RRB information resources and shall approve CERT membership as recommended by the Chief Security Officer (CSO). CIO responsibilities include:

- decision authority to disconnect or turn off mission critical systems ;
- ensuring the CERT is properly staffed and equipped to perform its functions;
- ensuring an appropriate level of protection for all RRB information resources; and
- ensuring appropriate measures are in place to protect RRB information technology assets.

Chief of Information Resources Management

The Chief of Information Resources Management is the senior management representative for the CERT and coordinates and assists in resolving any incident response issues with other senior managers in the RRB, including escalating issues to the CIO for action if required. The Information Resources Management Center includes the Risk Management Group. The Risk Management Group, headed by the CSO, is responsible for providing a standard, systematic, enterprise-wide process for risk management.

Chief Security Officer

The CSO has operational authority over the CERT and coordinates with managers including the CIO and Chief of Information Resources Management. CSO responsibilities include:

- ensuring the RRB policy and procedures conform to the requirements of Federal laws and regulations;
- promulgates additional policy and procedures as necessary to provide for adequate computer security;
- recommends CERT members to the CIO for approval;
- translates technical details of incidents into business impact statements for the benefit of senior, non-technical management;
- advises the CIO of the potential impact an incident could have on business operations;
- ensures that a computer security incident reporting systems is developed, implemented, monitored and evaluated;
- evaluates and activates the CERT on suspected security intrusion, incidents or violations reported from the BIS Customer Services Support Group; and
- recommends corrective measures and solutions to prevent or resolve computer security related incidents.

Lead Investigator (LI)

The LI is authorized by the CIO to lead the CERT in conducting authorized computer incident investigations. The LI is normally a member of the CSO's staff unless criminal involvement is suspected or discovered, in which case the Office of Inspector General's Office of Investigations assumes responsibility. The LI, in cooperation with the CERT, is responsible for responding to suspected or actual incidents in a timely manner. The LI may need to perform highly complex tasks, and is expected to have a high level of technical expertise. The LI undergoes comprehensive training in the tools and techniques of incident response and computer forensics. LI responsibilities include:

- managing and directing the incident response team, including periodic training;
- serving as a link between management and the incident response team;
- informing the CSO of CERT actions;

- submitting incident reports, both internally and externally;
- maintaining the Computer Security Incident Response Plan procedures;
- selecting and using incident response tools, including a separate forensics workstation; and
- installing, configuring, and using the RRB intrusion detection/prevention tools.

Network Engineer (NE)

The NE plays a pivotal role on the CERT by assisting the LI with specific tasks, including collecting detailed data about the state of an affected system when an incident occurs. Often, the NE is involved at the earliest stages of an incident and may be the first person to detect when an incident occurs. The NE is a staff member of the Network Services Group and is responsible for:

- ensuring that RRB system security conform to best practices;
- securing RRB systems to prevent intrusions and unauthorized access;
- ensuring all RRB general support systems are secured and patched in accordance with RRB policy;
- generating and collecting detailed audit logs as prescribed by the LI;
- monitoring and validating user account activity;
- configuring system security settings in accordance with RRB policy; and
- performing administrative functions on key infrastructure components such as domain name systems, network attached storage, email, web, and antivirus servers.

Data Communications Engineer (DCE)

The DCE plays a significant role on the CERT by ensuring that the network devices (routers, switches, firewalls, and virtual private network implementations) are secured. The DCE may be the first person to recognize a potential incident requiring further investigation. The DCE is a staff member of the Network Services Group and is responsible for:

- configuring network devices to ensure appropriate level of protection;
- securing the RRB internetworking systems to prevent intrusions and unauthorized accesses according to best practices of the profession;
- ensuring all RRB network devices are secured and patched in accordance with RRB policy;
- enabling and configuring logging on critical network devices;
- generating and collecting detailed audit logs as prescribed by the LI;
- monitoring network activity for anomalous or suspicious activity; and
- coordinating with providers as required by Service Level Agreements.

Customer and Desktop Support Services Groups (CSSG/DSSG)

The CSSG/DSSG, within the Network Services Group, is the primary point of contact for all user initiated computer security incident reporting. They are responsible for manning the RRB's Help Desk functions and ensuring individual workstations have been secured and patched in accordance with RRB policy. Upon recognition of an incident, the CSSG/DSSG will determine whether the affected system poses a significant security threat to the agency, and if so, takes appropriate actions to isolate the affected system(s).

APPENDIX II

RRB CERT MEMBER'S ROLES AND RESPONSIBILITIES

System Security Specialist (SSS)

The SSS is responsible for all user related account functions and permissions for both the mainframe and end user computing systems. The SSS is likely the first person to notice questionable user account activity during routine auditing functions. Other indicators of a computer security incident involving the SSS are forwarded by a user who notices a problem with their account. The SSS is also responsible for the internet web filtering application and may detect incidents involving unauthorized employee internet activity. The SSS is a staff member of the Network Services Group.

Mainframe Computer Supervisor and Staff (MCSS)

The MCSS is the primary technical point of contact for all mainframe related security issues. Their expertise and support is critical in determining if the mainframe or data has been compromised during a computer security incident, specifically in those incidents when the mainframe is suspected of being the primary target. The mainframe system is the RRB's principal and critical line of business system.

Database Administrator (DA)

The DA is the primary technical point of contact for all database related issues, regardless of what platform the data resides on (mainframe or end-user computing). The DA has the technical expertise to help identify if an RRB database has been compromised, and if so, can provide a damage assessment and recommended corrective actions.

Web Administrator (WA)

The WA is responsible for all internet and intranet applications and proper hosting and access to RRB websites, both internal and external. The WA provides the coordination linkage with the E-Government developers, as well as with the contracted web hosting vendor.

Various Intra-agency Line-of-Business Staff

Each major application has been appointed an Information System Security Officer and Line of Business manager who are responsible for providing technical and business impact support to the CERT effort as needed.

APPENDIX III

GLOSSARY

Antivirus Software: A program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents.

Firewall: A program that protects a computer or network from other networks by limiting and monitoring network communications.

Hot fix: Microsoft's term for a security patch.

Intrusion Detection System (IDS): Software that looks for suspicious activity and alerts administrators.

Intrusion Prevention System: A program that performs packet sniffing and analyzes network traffic to identify and stop suspicious activity. Intrusion Prevention Systems may also be host-based.

Malicious code: A virus, worm, Trojan horse, or other code-based entity that infects a host.

Malware: A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.

Patch: An additional piece of code developed to address a problem in an existing piece of software.

Patch Management: The process of acquiring, testing, and distributing patches to the appropriate administrators and users throughout the organization.

Phishing: Tricking individuals into disclosing sensitive personal information through deceptive computer-based means.

Quarantining: Storing files containing malware in isolation for future disinfection or examination.

Router: A hardware device that allows data to be exchanged between networks. Routers are similar to bridges, but provide additional functionality, such as the ability to filter messages and forward them to different places based on various criteria.

Service pack: A method for conveniently bundling existing updates for a product. The bundle contains new features and enhancements in order to improve security, reliability and to improve administration.

Spam: To indiscriminately send unsolicited, unwanted, irrelevant, or inappropriate messages, especially commercial advertising in mass quantities. Noun: electronic "junk mail".

Spyware: Stand-alone programs that can secretly monitor system activity and detect passwords and other confidential information and relay it back to another computer.

Switch: In networks, a device that filters and forwards packets between LAN segments. Switches support any packet protocol.

Threat: Any circumstance or event, deliberate or unintentional, with the potential for causing harm to a system.

APPENDIX III

GLOSSARY

Trojan horse: A nonself-replicating program that seems to have a useful purpose, but in reality has a different, malicious purpose.

Virus: A program designed with malicious intent that has the ability to spread to multiple computers or programs. Most viruses have a trigger mechanism that defines the conditions under which it will spread and deliver a malicious payload of some type. Some viruses specifically damage data by corrupting programs, deleting files, or reformatting disks.

Virus Definition Files: Files that contain sample code for thousands of threats. When antivirus software scans a computer, it attempts to find matches between the computer's files and the sample code inside the virus definition file. When a match is found, it is an indication that the file has been infected.

VPN (Virtual Private Network): A network where packets that are internal to a private network pass across a public network. In a secure VPN, traffic is encrypted, integrity protected and encapsulated into new packets that are sent across the Internet.

Vulnerability: A weakness in a system, application, or network that is subject to exploitation or misuse.

Worm: A type of malicious code particular to networked computers. It is a self-replicating program that works its way through a computer network exploiting vulnerable hosts, replicating and causing whatever damage it was programmed to do.

UNITED STATES GOVERNMENT

MEMORANDUM

FORM G-115f (1-92)

RAILROAD RETIREMENT BOARD

August 17, 2006

TO : Henrietta B. Shaw
Assistant Inspector General, Audit

FROM : Terri S. Morgan
Chief Information Officer

SUBJECT: Draft Report – Review of Incident Handling and Reporting at the Railroad Retirement Board, June 28, 2006

We have completed our review of the subject report and have the following comments.

Recommendation 1 – We recommend that the Bureau of Information Services conduct training of the RRB CERT members' roles and responsibilities.

BIS Response – We concur with this recommendation. CSIRP awareness training will be provided to all CERT members. Target completion date is September 29, 2007.

Recommendation 2 – We recommend that the Bureau of Information Services implement controls to ensure the continued adherence to, and usefulness of the CSIRP procedures.

BIS Response – We concur with the recommendation and have adopted the updated list of controls based upon the NIST baseline requirements specified in SP800-53 that includes Incident Response checks.

Recommendation 3 – We recommend that the Bureau of Information Services develop a formal antivirus configuration policy.

BIS Response – We accept this recommendation. There are 2 antivirus servers at the RRB. We keep the servers at the current level recommended by Symantec. Servers are updated per Symantec notifications and are performed along with the Microsoft updates on the 3 or 4 weekend of each month.

Recommendation 4 – We recommend that the Bureau of Information Services implement procedures for adequately documenting and approving deviations from that policy;

BIS Response – We accept this recommendation. Network administrators are working with Symantec to create the reports to be used to document the history of the Server Anti-Virus updates and configurations. Similar to Microsoft updates, these documents record the status of each server. Any deviation will be recorded. Target date for completion is September 2006.

Recommendation 5 – We recommend that the Bureau of Information Services appoint a backup administrator for managing the antivirus software.

BIS Response – We accept this recommendation. ISC has 2 network administrators who have been trained and are designated as Norton Anti Virus administrators. Staff assignments were given in February 2006.

Recommendation 6 – We recommend that the Bureau of Information Services provide adequate training to the new antivirus administrator and backup administrator.

BIS Response – We accept this recommendation. ISC has 2 network administrators who have been trained and are designated as Norton Anti Virus administrators. Training to both Anti-Virus administrators was given in June 2006.

Recommendation 7 – We recommend that the Bureau of Information Services implement controls to ensure incident reports released to US-CERT are complete, accurate, and conform to US-CERT requirements

BIS Response – We conditionally accept recommendation. We have implemented additional controls to ensure that incident reports released to US-CERT are complete and accurate, however the US-CERT requirement for a daily reporting of successful virus infections is unrealistic and at the moment unachievable for the RRB. Effective reporting cannot even begin until recommendations 3 to 6 above are fully implemented. Additionally, a linkage between the Anti-Virus (A-V) administrator and the help desk ticketing software is required to provide timely and documented A-V response. When established the A-V administrator will be responsible for daily reporting to RRB and US-CERT.

(Although requested several times, US-CERT has yet to provide a point of contact for their Continuity of Operations (CONOPS) manual. The CONOPS manual contains the report reporting requirements. Additionally, US-CERT has not answered our requests for how many federal agencies effectively report daily malicious code infections.)

Recommendation 8 – We recommend that the Bureau of Information Services implement a system to track and communicate all incidents, including successful malicious code identified by the antivirus software, from discovery to completion and final reporting.

BIS Response – We accept this recommendation. Network Administrators are working with Symantec to document all occurrences noted by the Anti-Virus application. We are actively trying to create the documents requested. We have been in contact with Symantec to help us resolve the reporting issues. Completion of this is targeted for September 2006.

Recommendation 9 – We recommend that the Bureau of Information Services implement controls to ensure internal reports of incidents are accurate and complete.

BIS Response – We concur with the recommendation and have adopted the controls specified in NIST SP 800-53, Recommended Security Controls for Federal Information Systems.

Recommendation 10 – We recommend that the Bureau of Information Services issue reports of major incidents to RRB management as soon as the nature of the incident is known, rather than when recommendations for future actions are implemented.

BIS Response – We concur with this recommendation. No additional changes required. Reports will be provided to management as required; normally these are oral crisis management briefings, electronic mail or slides. A formal report is prepared at the end of the incident. The CSIRP will be updated to reflect that the final report is due to the CIO within 60 days of the incident closure. Target date for completion is November 30, 2006.

Recommendation 11 – We recommend that the Bureau of Information Services develop and implement a formal policy and procedure addressing patch management.

BIS Response – Bureau of Information Services has agreed to this recommendation and documentation was submitted to OIG on August 7, 2006 to support implementation.