



*The Office of Research, Analysis, and
Statistics Needs to Address Computer
Security Weaknesses*

September 17, 2008

Reference Number: 2008-20-176

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

Redaction Legend:

3(d) = Identifying Information - Other Identifying Information of an Individual or Individuals



TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

September 17, 2008

MEMORANDUM FOR DIRECTOR, OFFICE OF RESEARCH, ANALYSIS, AND
STATISTICS

FROM: *Michael R. Phillips*
Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The Office of Research, Analysis, and Statistics
Needs to Address Computer Security Weaknesses (Audit # 200720032)

This report presents the results of our review to determine whether the Internal Revenue Service's (IRS) Office of Research, Analysis, and Statistics (RAS organization) maintained effective security controls over its information systems. This review was included in the Treasury Inspector General for Tax Administration Fiscal Year 2008 Annual Audit Plan and was part of the Information Systems Programs business unit's statutory requirement to annually review the adequacy and security of IRS technology.

Impact on the Taxpayer

Information technology personnel in the RAS organization manage computer systems containing a significant amount of sensitive taxpayer data. Users query these systems to obtain enormous amounts of taxpayer data. However, these personal data were not adequately secured. Several security weaknesses existed on each of the three computer systems we reviewed. These weaknesses increase the risks of 1) unauthorized disclosure of taxpayer data that could be used for identity theft, and 2) significant disruption to computer operations.

Synopsis

The RAS organization is the main provider of statistics about the Federal Government tax system. It also provides IRS officials with a suite of research tools and comprehensive analyses to support management decisions.



*The Office of Research, Analysis, and Statistics Needs to
Address Computer Security Weaknesses*

We identified several weaknesses over the management of access to the RAS organization's computer systems. Managers did not carry out their responsibilities to ensure that 1) users were authorized to access the computer systems, 2) access accounts for former employees and current employees who no longer needed access were removed, and 3) system administrators removed or locked unnecessary generic or shared administrator accounts that provide additional opportunities for malicious intruders to gain access to the systems.

In addition, password settings did not conform to IRS information security standards. For example, passwords were not always sufficiently complex, passwords were not set to expire after the required length of time, and new users were not required to change their passwords at initial login.

Unencrypted sensitive data were transferred between computers. The IRS has developed procedures to limit unsecured services on its networks and was in the process of implementing these procedures during our review. However, the unsecured services were still in use on the RAS organization's computer systems.

Controls to detect inappropriate security events were not effective. Audit log¹ data were not adequately retained or reviewed on the computer systems. Intrusion detection systems were not installed and virus protection software was not current. In addition, data received from other sources were not scanned with virus protection software before being uploaded to the server.

The IRS requires that system backup files be stored offsite. However, offsite storage was not used for backup files because the RAS organization had not completed negotiations with the IRS Modernization and Information Technology Services organization to secure the system backup files.

We also identified database security vulnerabilities within the systems we reviewed. Database patching² was not adequate, access permissions were set incorrectly, password settings were incorrect, and the auditing feature was not properly enabled to detect unauthorized activities in the databases.

Our findings indicate that managers and system administrators had not placed sufficient emphasis on maintaining the security and privacy of the taxpayer data they were charged with protecting. In addition, a security officer had not been designated to communicate security guidance and monitor compliance with IRS security policies, and software was not available to scan for security weaknesses. Until these root causes are addressed, the RAS organization will be unable to effectively manage and secure systems containing taxpayer identifiable information.

¹ An audit log is a chronological record of system activities that allows for the reconstruction, review, and examination of a transaction from inception to final results.

² A patch is a fix of a design flaw in a computer program. Patches must be installed or applied to the appropriate computer for the flaw to be corrected.



The Office of Research, Analysis, and Statistics Needs to Address Computer Security Weaknesses

Recommendations

We recommended that the Director, Office of Research, Analysis, and Statistics, 1) designate a security officer to monitor compliance with IRS security requirements and remind managers and employees of their security responsibilities, 2) require system administrators and their managers to ensure that all system access controls are followed, and to follow up on identified security weaknesses to ensure they are corrected in a timely manner, 3) coordinate with the Modernization and Information Technology Services organization to implement secure processes for transferring sensitive data between computers, and ensure that scanning software is used to periodically scan the RAS organization's systems for security weaknesses, 4) implement and monitor a process by which managers validate that system access is limited to only those who have a need, 5) ensure that audit and accountability controls are sufficient by requiring that audit logs are maintained a minimum of 6 years and are reviewed by the security officer, 6) require managers to ensure that offsite storage is used for system and data backup files, and 7) coordinate with the Chief Information Officer to verify that intrusion detection systems are installed to protect all systems and that virus protection software is current.

Response

The Director, Office of Research, Analysis and Statistics, agreed with our recommendations and informed us that many of their corrective actions have already been taken. The RAS organization will 1) designate a security officer and require system administrators and their managers to follow system access controls, 2) follow up on identified security weaknesses and ensure they are tracked on a Plan of Action and Milestones³ and corrected in a timely manner, 3) work with the Modernization and Information Technology Services organization to ensure that data files are transmitted securely between computers as soon as an alternate data transfer service is available, and ensure that scanning software is used to periodically scan the systems for security weaknesses, 4) periodically review system access records for all systems to validate that access is granted on a need-to-know basis, 5) retain audit logs for 6 years and require that the newly designated security officer review the audit logs, 6) continue coordinating with the IRS Enterprise Operations office to have the system and data backup files stored offsite, and 7) continue coordinating with the Modernization and Information Technology Services organization to install host intrusion detection software and virus protection software on all

³ A Plan of Action and Milestones, also referred to as a corrective action plan, is a tool that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the Plan, any milestones in meeting the task, and scheduled completion dates for the milestones.



*The Office of Research, Analysis, and Statistics Needs to
Address Computer Security Weaknesses*

systems as soon as available. Management's complete response to the draft report is included as Appendix V.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions or Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs) at (202) 622-8510.



*The Office of Research, Analysis, and Statistics Needs to
Address Computer Security Weaknesses*

Table of Contents

Background	Page 1
Results of Review	Page 3
The Office of Research, Analysis, and Statistics Needs to Implement Adequate Security Controls	Page 3
<u>Recommendations 1 and 2:</u>	Page 9
<u>Recommendations 3 and 4:</u>	Page 10
<u>Recommendations 5 through 7:</u>	Page 11
Appendices	
Appendix I – Detailed Objective, Scope, and Methodology	Page 12
Appendix II – Major Contributors to This Report	Page 14
Appendix III – Report Distribution List	Page 15
Appendix IV – Description of the Office of Research, Analysis, and Statistics Suboffices	Page 16
Appendix V – Management’s Response to the Draft Report	Page 17



*The Office of Research, Analysis, and Statistics Needs to
Address Computer Security Weaknesses*

Abbreviations

IRS	Internal Revenue Service
RAS organization	Office of Research, Analysis, and Statistics



*The Office of Research, Analysis, and Statistics Needs to
Address Computer Security Weaknesses*

Background

The Internal Revenue Service's (IRS) Office of Research, Analysis, and Statistics (RAS organization) is the main provider of statistics about the Federal Government tax system. It also provides IRS, Department of the Treasury, and other Federal Government officials with a suite of research tools to conduct comprehensive analyses.

The statistical data and analyses provided by the RAS organization allow the IRS to prepare studies, evaluate tax programs and initiatives, and respond to information requests from Congress and other stakeholders. Examples of analyses conducted by the RAS organization include statistics on taxpayers' voluntary compliance with tax laws, enforcement activities conducted by the IRS, and electronic filing trends. During Fiscal Year 2007, various organizations made more than 1,700 research requests for data stored on the RAS organization's computer systems.

The taxpayer data include information obtained from the following major IRS data sources:

- Individual Master File – The IRS database that maintains transactions or records of individual tax accounts.
- Business Master File – The IRS database that consists of Federal tax-related transactions and accounts for businesses. These include employment taxes, income taxes on businesses, and excise taxes.
- Audit Information Management System – The IRS system that processes information related to IRS examinations of taxpayers.

The RAS organization is comprised of five suboffices: Office of Research, National Research Program office, Office of Program Evaluation and Risk Analysis, Statistics of Income Division, and Office of Servicewide Policy Directives and Electronic Research. A detailed description of each suboffice is included in Appendix IV.

The RAS organization operates three main computer applications to accomplish its mission:

- **Compliance Data Warehouse** – Provides access to a wide variety of tax return, enforcement, compliance, and other data to support the query and analysis needs of the research community. It captures data from multiple production systems and migrates, transforms, and organizes the data in a way that is conducive to analysis.
- **Statistics of Income Distributed Processing System** – Supports the IRS requirement to annually report to Congress on the numbers and types of tax returns filed and the characteristics and money amounts reported on those returns. The sample data are used



The Office of Research, Analysis, and Statistics Needs to Address Computer Security Weaknesses

by the Bureau of Economic Analysis, the Congressional Budget Office, the Department of the Treasury Office of Tax Analysis, and the Joint Committee on Taxation.

- **YK1 Link Analysis Tool** – Extracts data from an Oracle database that contains selected information from the Individual¹ and Business Master File Returns Transaction Files.² The application uses partnership data to show how gains and losses flow through and across all related entities.

We focused our review on technical, operational, and managerial controls that should be established to protect these three applications, which we refer to as “systems” in this report. The RAS organization employs its own Information Technology function to manage the security over its Statistics of Income Distributed Processing System. The security controls for the Compliance Data Warehouse and the YK1 Link Analysis Tool systems are managed jointly by the RAS organization and the IRS Modernization and Information Technology Services organization. This arrangement is in contrast to the majority of IRS organizations, whose computer systems are administered by the Modernization and Information Technology Services organization.

This review was performed in the RAS organization offices in Washington, D.C., and the Ogden, Utah, Campus³ during the period August 2007 through April 2008. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

¹ Individual Return Transaction File programs receive individual tax return data, reformat, and post returns to the Return Transaction On-Line File. They also do weekly cross-reference maintenance.

² Business Return Transaction File programs receive business tax return data, reformat, and post returns to the Return Transaction File, and do periodic file maintenance.

³ Campuses are the data processing arm of the IRS. They process paper and electronic submissions, correct errors, and forward data to the Computing Centers for analysis and posting to taxpayer accounts.



*The Office of Research, Analysis, and Statistics Needs to
Address Computer Security Weaknesses*

Results of Review

The Office of Research, Analysis, and Statistics Needs to Implement Adequate Security Controls

Information technology personnel in the RAS organization manage computer systems containing a large amount of sensitive taxpayer data. To accomplish their missions, system users must be able to access enormous amounts of taxpayer data. The risk of unauthorized disclosure of these data dictates tight control and close monitoring to ensure that security vulnerabilities are identified and corrected in a timely manner. However, we found significant security weaknesses on each of the RAS organization's computer systems reviewed. These weaknesses increase the risks of 1) unauthorized disclosure of taxpayer data that could be used for identity theft, and 2) significant disruption to computer operations.

Our findings indicate that managers and system administrators had not placed sufficient emphasis on maintaining the security and privacy of the taxpayer data they are charged with protecting. In addition, a security officer had not been designated to communicate security guidance and monitor compliance with IRS information security policies, and software was not available to scan for security weaknesses. Until these root causes are addressed, the RAS organization will be unable to effectively manage and secure systems containing taxpayer identifiable information.

Management of access to systems was inadequate

Each employee and contractor request for access to a system should be authorized by his or her manager using an Information System User Registration/Change Request (Form 5081). Before authorizing an employee or contractor to have access to a system, the manager should ensure that the potential user needs the access to carry out his or her responsibilities and has passed a background investigation. Managers are also required to annually review their employees' and contractors' access rights to ensure that the employees or contractors still need access to the computer system. As an added control, the IRS requires that systems be configured to disable a user's account if it has not been used in the last 45 calendar days and to remove the account from the system if it has not been used in the last 90 calendar days. Finally, to ensure accountability, system administrators who are responsible for maintaining the computer systems must log into their own unique accounts prior to accessing the systems and performing their duties.

We identified the following authorization control weaknesses:

- System administrators provided access to 67 (11 percent) of 613 employees and contractors on the 3 systems we reviewed without proper authorization from managers.



The Office of Research, Analysis, and Statistics Needs to Address Computer Security Weaknesses

For the YK1 Link Analysis Tool system, three users with administrative rights had not been authorized by a manager.

- System administrators had not configured the systems to disable and remove inactive accounts as required. We found 71 accounts on the Compliance Data Warehouse system and 31 accounts on the Statistics of Income Distributed Processing System that had not been accessed in more than 45 calendar days. Another 81 accounts had not been accessed on the Compliance Data Warehouse system, Statistics of Income Distributed Processing System, or YK1 Link Analysis Tool system in more than 90 calendar days.
- Managers had not advised system administrators to remove the accounts of 17 former employees who had access to a RAS organization system.
- Managers failed to confirm that background investigations were completed on each user prior to granting users access to the systems. We found six users had access to the systems, but managers in the RAS organization did not verify that background investigations had been completed prior to their receiving system access.
- Managers permitted the use of 4 and 11 generic or shared administrator accounts, respectively, on the Compliance Data Warehouse system and the Statistics of Income Distributed Processing System. Because these accounts contain powerful authorities and present malicious intruders additional opportunities to access a system, the IRS requires that these accounts be removed or disabled.

- **3(d)** [redacted] which is the most powerful account on the computer system. To ensure accountability for actions taken on computer systems, IRS security procedures require system administrators to first log on a system with their personal account before using the sensitive permissions of the "root" account. This procedure provides unique identification and allows management to identify which system administrator used the "root" account and to determine what actions he or she executed. By not logging into a personally identifiable account [redacted] **3(d)** [redacted] If an intruder or hacker were to gain access to the root account, management would be unable to distinguish the actions of the intruder from those performed by the system administrator.

We attribute these weaknesses to several causes. Specifically:

- Managers did not carry out their responsibilities for ensuring that their employees and contractors were authorized to access the RAS organization systems.
- Managers of system administrators did not provide sufficient oversight to ensure that the administrators followed IRS security procedures, and, in some cases, managers were unaware of the risks associated with noncompliance with these



*The Office of Research, Analysis, and Statistics Needs to
Address Computer Security Weaknesses*

procedures. These control weaknesses increase the risk that an unauthorized or malicious person could gain access to the systems to steal taxpayer information or disrupt operations.

Users' passwords did not comply with IRS standards

To ensure that employees and contractors are who they say they are, the IRS requires each user to have a unique password. The IRS also provides specific requirements for passwords to ensure that they are sufficiently complex so they cannot be easily guessed. Password settings on the Compliance Data Warehouse and the YK1 Link Analysis Tool systems did not conform to IRS information security standards. For the Compliance Data Warehouse system, the passwords were not always sufficiently complex, the passwords were not set to expire after the required length of time, and new users were not required to change their passwords when they initially login. On the YK1 Link Analysis Tool system, passwords were not set to expire after the required length of time.

System administrators stated that they were unaware of certain password standards. In addition, their managers did not provide sufficient oversight to ensure that the administrators were complying with IRS standards. Malicious users can exploit user accounts with weak password settings to steal taxpayer identities and carry out fraud schemes.

Unencrypted sensitive data were transferred between computers

The IRS developed procedures to limit unsecured services on networks. However, these services were still in use. We identified two high-risk, inadequately configured computer services running on all of the systems. Specifically, the File Transfer Protocol and the Telnet services were used to facilitate remote transfers of taxpayer data and provide remote access to computers containing taxpayer identifiable information. The use of these two services is widely known in the information technology industry as being insecure because they do not encrypt data transferred between computers.

The RAS organization's Internet web site states that the Compliance Data Warehouse system supports the use of the File Transfer Protocol on a temporary basis, usually for a period not to exceed 10 business days. This allows a fast, convenient method for transferring larger amounts of data to and from the Compliance Data Warehouse system environment. However, according to the IRS information security policy, these types of services should be prohibited.

The IRS was in the process of implementing secure methods for transferring sensitive data during our review. However, RAS organization managers had not yet implemented those methods. As a result, the risks of unauthorized access to and disclosure of highly sensitive taxpayer data transmitted between RAS organization systems were increased.



*The Office of Research, Analysis, and Statistics Needs to
Address Computer Security Weaknesses*

System backups were not stored at an offsite facility

The IRS requires that system backup files be stored offsite. However, offsite storage was not used for backup files for the systems we reviewed. Previously, the IRS National Headquarters had been selected as the offsite storage facility for the RAS organization's systems. This arrangement was terminated after the National Headquarters was damaged by a flood in June 2006.

During our review, the RAS organization was negotiating with the Modernization and Information Technology Services organization to obtain offsite storage. However, the RAS organization did not place sufficient emphasis on implementing this security control and the negotiations were not completed. Failure to use offsite storage could result in an inability to recover key data in the event of a disaster.

System audit logs were not always retained or reviewed

IRS procedures state that each computer system is required to collect and review audit log information at least weekly. Audit logs should be retained for 6 years. An audit log is defined as a chronological record of system activities that allows for the reconstruction, review, and examination of a transaction from inception to final results. Audit logs are essential in determining accountability for unauthorized use of or changes to a system, investigating security incidents, and monitoring user and system activities.

Audit logs for the RAS organization's computer systems were not adequately retained or reviewed. For example, audit log data were not adequately retained on the Statistics of Income Distributed Processing System. On the YK1 Link Analysis Tool system, audit trail data were retained and reviewed. However, administrator actions and configuration changes were not included in the review. Audit logs for the Compliance Data Warehouse system had been retained but were not regularly reviewed.

The RAS organization did not designate a security officer to review audit logs and report security weaknesses to management. When audit log data are not reviewed, improper activities carried out by external intruders or malicious internal users are less likely to be detected.

Intrusion detection systems were not installed, and virus protection software was not current

The IRS recommends use of intrusion detection systems and virus protection software to deter and detect unauthorized users from entering or disrupting IRS operations. Intrusion detection systems can inspect all inbound and outbound network activity and identify suspicious patterns that might indicate a network or system is being attacked. Intrusion detection systems were not installed on the three systems we reviewed. Also, virus protection software was not current on the Statistics of Income Distributed Processing System. In addition, data received from other sources were not scanned with virus protection software before being uploaded to the server.



*The Office of Research, Analysis, and Statistics Needs to
Address Computer Security Weaknesses*

Although this is not a requirement and the data are generally received from trusted sources, the damage that can be caused by viruses and worms on systems containing large amounts of data, as in the RAS organization's systems, indicates the need to scan the data from other sources before loading the data onto the systems.

Managers and system administrators had relied on Modernization and Information Technology Services organization staff to implement intrusion detection systems and virus protection software. However, the RAS organization's managers and system administrators did not follow up to ensure that these controls were implemented. The lack of intrusion detection systems and current virus protection software increases the risk that data could be stolen and computer operations disrupted.

Database scanning revealed numerous high-risk vulnerabilities

Our review focused primarily on security controls to protect the RAS organization's computer systems. However, because databases are part of the systems and hackers could gain access to taxpayer data in the databases without entering the systems, we also tested security controls specifically related to the databases. While the security of sensitive taxpayer data is dependent on the strength and layers of the security controls protecting it, the last and possibly best line of defense is a system of database security controls.

We identified the following database security vulnerabilities on all three of the systems:

- The database administrators did not adequately install updates and patches⁴ to the databases, as evidenced by our scanning results. Database vendors often discover security weaknesses in their databases after their products are sold to customers. To address the security weaknesses, the vendors issue patches or updates to their customers. When vendors issue security patches, they are acknowledging that their products contain security vulnerabilities that can be exploited. However, issuing patches also notifies the hacker community of potential security vulnerabilities, often causing a race between hackers attacking these vulnerabilities and information technology professionals installing the patches on their systems. The National Institute for Standards and Technology⁵ states that, "Timely patching is critical to maintain the operational availability, confidentiality, and integrity of Information Technology systems. However, failure to keep operating systems and system software patched is the most common mistake made by Information Technology professionals."⁶ National Institute for

⁴ A patch is a fix of a design flaw in a computer program. Patches must be installed or applied to the appropriate computer for the flaw to be corrected.

⁵ The National Institute of Standards and Technology, under the Department of Commerce, is responsible for developing standards and guidelines for providing adequate information security for all Federal Government agency operations and assets.

⁶ *Creating a Patch and Vulnerability Management Program* (National Institute for Standards and Technology Special Publication 800-40, dated November 2005).



*The Office of Research, Analysis, and Statistics Needs to
Address Computer Security Weaknesses*

Standards and Technology guidance directs that organizations should regularly check for updates and patches from vendors and apply them in a timely manner, and scan systems to validate whether security patches and software versions are current.

- The database administrators did not adequately restrict database access permissions. The IRS requires that database access permissions be configured based on the principle of least privilege. Users should be granted the least and weakest privileges needed to perform their duties. For example, some users have the sole need of reading the data. Therefore, the database administrator should configure the database access permissions to ensure that these users cannot delete data or execute powerful database functions. The database administrators did not adhere to the principle of least privilege in granting privileges to the “Public” access permission, which is automatically given to all users during database installation. The excessive privileges granted to the Public access permission could be used to circumvent database security and corrupt the computer system. Users in the Public group could also unintentionally modify or delete database tables that are needed by the systems to generate accurate analyses and statistics.
- The database administrators did not establish password settings in compliance with IRS standards. They did not establish settings to ensure that 1) default passwords were changed after initial login, 2) the minimum password length was set to the required number of characters rather than zero, and 3) the number of failed login attempts before users were locked out of the system was correct.
- The database administrators did not properly enable the auditing feature to detect unauthorized activities in the databases. The IRS requires that the auditing feature be active to track user activities within databases.

The above vulnerabilities resulted from a lack of attention to security by the RAS organization. In addition, the RAS organization informed us that it does not have database scanning software to detect the vulnerabilities we found with our scanning software. Had the RAS organization used database scanning software and implemented regular database scanning, these security vulnerabilities could have been identified and corrected in a timely manner.

The security vulnerabilities we detected provide an opportunity for data stored in the databases to be compromised, which could lead to identity theft or fraud. In addition, employees and intruders who gain unauthorized access to the systems and networks can cause major disruptions of service affecting productivity.



***The Office of Research, Analysis, and Statistics Needs to
Address Computer Security Weaknesses***

Recommendations

To address the security weaknesses we identified, the Director, Office of Research, Analysis, and Statistics, should:

Recommendation 1: Designate a security officer responsible for monitoring compliance with IRS security requirements and for reminding managers and employees of their security roles and responsibilities.

Management's Response: The RAS organization agreed with this recommendation. 3(d) employees in the RAS organization, 3(d) will immediately handle the security responsibilities until a permanent security officer is selected. The RAS organization is in the process of recruiting a security officer. Funding will be set aside to hire and train a security officer.

Recommendation 2: Require system administrators and their managers to:

- Disable accounts that have not been accessed in more than 45 calendar days.
- Remove accounts that have not been used in more than 90 calendar days.
- Remove or lock unnecessary generic and shared administrator accounts, and remove former employee accounts.
- Take actions to detect and prevent users from sharing login accounts.
- Log into their personal accounts with their own unique login identification and password prior to accessing a system's "root" account.
- Follow up on identified security weaknesses to ensure that they are corrected in a timely manner.

Management's Response: The RAS organization agreed with this recommendation. The RAS organization has disabled accounts that have not been accessed in more than 45 days on the Statistics of Income Distributed Processing System and the Compliance Data Warehouse system. For the YK1 system, the RAS organization is devising an automated email reminder system to alert users that their accounts will be disabled if the accounts are not accessed within 45 days. The RAS organization will test this new application and deploy it by the end of Calendar Year 2008. Upon deployment of the alert system, the RAS organization will begin disabling accounts that have not been accessed after a 45-day period.

The RAS organization will develop and implement a policy of removing user accounts on the Compliance Data Warehouse and YK1 systems that have not been used in more than 90 days.

The RAS organization will remove or lock all unnecessary generic or shared administrator accounts on the Compliance Data Warehouse and YK1 systems. For the Statistics of Income Distributed Processing System, many of the accounts had been



***The Office of Research, Analysis, and Statistics Needs to
Address Computer Security Weaknesses***

removed or disabled during the course of the our audit. The remainder will be analyzed and removed or locked. All user accounts of former employees on all three of the RAS organization systems have been removed, and a system will be put in place to ensure employees are removed from the systems as they terminate employment.

The RAS organization will implement a periodic review to identify and prevent users from sharing login accounts for the YK1 and Compliance Data Warehouse systems.

The RAS organization has resolved the issue of (b)(7)(D)

The RAS organization will follow up on identified security weaknesses to ensure the weaknesses are corrected in a timely manner. All identified security weaknesses will be tracked on a Plan of Action and Milestones for the system.

Recommendation 3: Coordinate with the Modernization and Information Technology Services organization to:

- Implement secure methods of transferring sensitive data between computers.
- Ensure that scanning software is used to periodically scan the RAS organization's systems for security weaknesses.

Management's Response: The RAS organization agreed with this recommendation. The RAS organization is now using secure file transfer protocol and secure shell to transfer data between the Compliance Data Warehouse and YK1 computer systems. In addition, the RAS organization is working with the Modernization and Information Technology Services organization to find an alternative secure method of transferring files from the Martinsburg Computing Center to the RAS organization systems.

The RAS organization will coordinate with the Modernization and Information Technology Services organization and the Computer Security Incident Response Center to ensure scanning software is used to periodically scan the systems for security weaknesses. In addition, the IRS Computer Security Incident Response Center currently performs security assessments of the RAS organization systems on a quarterly basis. The RAS organization will work with the Computer Security Incident Response Center to ensure recurring security assessments of the systems are performed and security vulnerabilities are remediated.

Recommendation 4: Remind managers to periodically review Form 5081 records to validate that access to systems is limited to only those who have a need. Managers should also be reminded to verify that potential users have received favorable background investigations before granting them access to systems.



The Office of Research, Analysis, and Statistics Needs to Address Computer Security Weaknesses

Management's Response: The RAS organization agreed with this recommendation. The RAS organization will periodically review Form 5081 records for all systems and use the online 5081 system to validate that system access is granted on a need-to-know basis. In addition, the RAS organization will not grant system access to employees without a favorable background clearance. Because the RAS organization relies on contractors to keep the Compliance Data Warehouse system running and background investigations are taking 6 months or longer to complete, system access will be restricted and Federal employees will closely monitor the work of contractors throughout regular working hours until the contractors receive a favorable background investigation.

Recommendation 5: Ensure that audit and accountability controls are sufficient by requiring that audit logs be maintained a minimum of 6 years and be periodically reviewed by the security officer.

Management's Response: The RAS organization agreed with this recommendation. Audit logs will be retained for 6 years and the newly designated security officer will review the audit logs.

Recommendation 6: Require managers to ensure that offsite storage is used for system and data backup files.

Management's Response: The RAS organization agreed with this recommendation. The RAS organization is currently working with the IRS Enterprise Operations office to have the RAS organization's system and data backup tapes included in the IRS' offsite storage contract.

Recommendation 7: Coordinate with the Chief Information Officer to verify that intrusion detection systems are installed on all systems and virus protection software is current.

Management's Response: The RAS organization agreed with this recommendation and is coordinating with the Modernization and Information Technology Services organization and Cybersecurity office to install host intrusion detection software. Virus protection software is being installed on all Windows-based servers and workstations. UNIX servers will have virus protection software installed once the software is purchased and made available by the Modernization and Information Technology Services organization.



*The Office of Research, Analysis, and Statistics Needs to
Address Computer Security Weaknesses*

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether the IRS RAS organization maintained effective security controls over its information systems. For the period August 2007 to April 2008, we evaluated compliance of three systems with specific technical, operational, and managerial controls required by the National Institute of Standards and Technology¹ and the IRS. These three systems were the Compliance Data Warehouse system, Statistic of Income Distributed Processing System, and YK1 Link Analysis Tool system. We also reviewed security controls on the databases within the systems. For any control deemed inadequate, we determined why and the effect of the inadequate control. To accomplish our objective, we:

- I. Determined whether key access controls were in place and operating effectively for each of the RAS organization's systems.
 - A. Determined whether accounts were reviewed at least annually to verify they were needed.
 - B. Determined whether generic, duplicate, or inactive accounts existed.
 - C. Evaluated technical database controls on the RAS organization's systems.
- II. Determined whether adequate audit logs were maintained, reviewed, and retained and whether adequate controls existed for ad hoc queries of taxpayer data.
 - A. Determined whether audit logs existed, captured key events, and were being reviewed.
- III. Determined whether authentication/password controls were in place and operating effectively.
 - A. Determined whether passwords met Internal Revenue Manual criteria.
- IV. Determined whether contingency plans existed and were tested for each of the three systems.
 - A. Determined whether system backups were stored offsite.

¹ The National Institute of Standards and Technology, under the Department of Commerce, is responsible for developing standards and guidelines for providing adequate information security for all Federal Government agency operations and assets.



*The Office of Research, Analysis, and Statistics Needs to
Address Computer Security Weaknesses*

- V. Determined whether key personnel controls were in place and operating effectively.
 - A. Determined whether user access privileges were removed from the system upon user termination.
 - B. Determined whether an Information System User Registration/Change Request (Form 5081) had been completed and approved for each system user.
 - C. Determined whether contractors or other third parties with system access had proper approvals and background checks completed prior to being given system access.
- VI. Determined whether system monitoring tools and security advisories were used.
 - A. Determined whether the systems used intrusion detection systems and virus protection software.
 - B. Determined whether the RAS organization received security advisories, issued alerts to staff, and took action based on alerts (e.g., installing current patches²).
- VII. Determined whether key certifications, accreditations, and security assessments were properly conducted and updated for each system.
 - A. Evaluated the adequacy of assessments and whether substantive testing was included as part of the assessments.
 - B. Determined whether Plans of Action and Milestones³ were developed and updated.
 - C. Determined whether the accreditation demonstrated adequate support for the accreditation decision.
- VIII. Determined whether risk assessments and vulnerability scanning were conducted for each system.

² A patch is a fix of a design flaw in a computer program. Patches must be installed or applied to the appropriate computer for the flaw to be corrected.

³ A Plan of Action and Milestones, also referred to as a corrective action plan, is a tool that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the Plan, any milestones in meeting the task, and scheduled completion dates for the milestones.



*The Office of Research, Analysis, and Statistics Needs to
Address Computer Security Weaknesses*

Appendix II

Major Contributors to This Report

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)
Preston B. Benoit, Acting Assistant Inspector General for Audit (Information Systems Programs)
Stephen Mullins, Director
Allen Gray, Audit Manager
Michelle Griffin, Audit Manager
Michael Howard, Audit Manager
Cari Fogle, Senior Auditor
Myron Gulley, Senior Auditor
Bret Hunter, Senior Auditor
Louis Lee, Senior Auditor



*The Office of Research, Analysis, and Statistics Needs to
Address Computer Security Weaknesses*

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Chief Information Officer OS:CIO
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Office of Internal Control OS:CFO:CPIC:IC
Audit Liaison: Director, Office of Research, Analysis, and Statistics RAS



*The Office of Research, Analysis, and Statistics Needs to
Address Computer Security Weaknesses*

Appendix IV

Description of the Office of Research, Analysis, and Statistics Suboffices

1. **Office of Research** – Improves tax administration by providing information, analysis, and solutions from an agency-wide perspective and by advocating actions for decision makers.
2. **National Research Program** – Measures voluntary compliance including filing, payment, and reporting compliance.
3. **Office of Program Evaluation and Risk Analysis** – Provides the senior leadership team with accurate and timely analysis of ongoing and proposed IRS programs and investments to support quality, data-driven strategic thinking and decision making across the organization.
4. **Statistics of Income Division** – Collects, analyzes, and disseminates information on Federal taxation for the Department of the Treasury Office of Tax Analysis, Congressional committees, IRS business units in their administration of the tax laws, other organizations engaged in economic and financial analysis, and the general public.
5. **Office of Servicewide Policy Directives and Electronic Research** – Designs and delivers core research tools and services that advance the customer service, compliance, and enforcement priorities of the IRS.



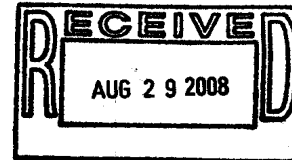
*The Office of Research, Analysis, and Statistics Needs to
Address Computer Security Weaknesses*

Appendix V

Management's Response to the Draft Report

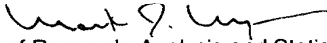


DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224



AUG 20 2008

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Mark J. Mazur 
Director, Office of Research, Analysis and Statistics

SUBJECT: Draft Audit Report – The Office of Research, Analysis, and
Statistics Needs to Address Computer Security Weaknesses
(Audit # 200720032)

This memorandum provides comments from the Internal Revenue Service (IRS) concerning the subject draft audit report. The IRS appreciates the time and effort that auditors from the Office of the Treasury Inspector General for Tax Administration (TIGTA) devoted to understanding our computer systems and the security controls on those systems. We agree with the report's recommendations, and will implement them to the extent the corrective actions fall within our control. One point we want to stress is that measures are now in place that address many of the concerns TIGTA had regarding Information Technology (IT) security in the Research, Analysis, and Statistics (RAS) organization. This TIGTA audit began over one year ago, and many security controls were being put in place across the entire IRS to meet rapidly changing security standards. Between the time the audit started and the time the draft report was released, Research, Analysis, and Statistics staff have taken many steps to upgrade and improve security to reduce the risk of unwarranted data disclosure.

Another point to note is that it is crucial for RAS and Modernization & Information Technology Services (MITS) to communicate effectively and partner productively. Several of the recommendations made by TIGTA can simply not be implemented without full MITS participation and cooperation. For example, the draft report noted that unencrypted data were transferred between computers. Much of this data transfer occurs from Martinsburg Computing Center (MCC) using File Transfer Protocol (FTP). However, unencrypted FTP cannot be disabled by MITS until there is a fully implemented secure substitute. RAS cannot implement a corrective action on this item without MITS support.

In summary, RAS is taking, and has been in the process of taking, the necessary steps to provide adequate security to the computer systems for which we are responsible, and address those issues within our control. We believe the RAS organization is taking the



*The Office of Research, Analysis, and Statistics Needs to
Address Computer Security Weaknesses*



DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

necessary actions to implement important security controls and effectively manage and secure systems containing taxpayer identifiable information.

Once again, we appreciate the opportunity to comment on the draft report. We believe we have already taken many steps to improve our IT systems' security posture. We expect that our actions to address the recommendations contained in this report will further strengthen our security situation and reduce the risk of inappropriate disclosure of tax data.

If you have any questions, please contact me at (202) 874-0100.

Our comments related to the report's specific recommendations follow.

RECOMMENDATION 1

Designate a security officer responsible for monitoring compliance with IRS security requirements and for reminding managers and employees of their security roles and responsibilities.

CORRECTIVE ACTION

- RAS management recognizes the need for adhering to IRS security requirements. We agree with the recommendation to designate a security officer to monitor compliance with IRS security requirements and remind managers and employees of their security roles and responsibilities. Currently, several of our employees have security roles in addition to responsibilities other than security. The RAS security officer position would be dedicated to complying with all the IRS security requirements. Constant communication with the various RAS offices and MITS would be essential. Funding will be set aside for this position and required training.

IMPLEMENTATION DATE

IT security duties will immediately be handled by one employee in SOI, a certified security specialist, and one in the Office of Research, who will assume these duties until the selection of a Security Officer. We are now beginning a recruiting action for this position and expect to have a Security Officer on board by March 31, 2009.

RESPONSIBLE OFFICIAL

Director, Research, Analysis, and Statistics

CORRECTIVE ACTION MONITORING PLAN

Monitoring will be conducted as part of the regular reporting within the organization.



**The Office of Research, Analysis, and Statistics Needs to
Address Computer Security Weaknesses**



DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

RECOMMENDATION 2

Require system administrators and their managers to:

- Disable accounts that have not been accessed in more than 45 calendar days.
- Remove accounts that have not been used in more than 90 calendar days.
- Remove or lock unnecessary generic or shared accounts and remove former employee accounts
- Take actions to detect and prevent users from sharing login accounts.
- Log into their personal accounts with their own unique login identification and password prior to accessing a system's "root" account.
- Follow up on identified security weaknesses to ensure that they are corrected in a timely manner.

CORRECTIVE ACTION

- RAS has disabled accounts that have not been accessed in more than 45 days on the SOI-DPS and Collection Data Warehouse (CDW) systems reviewed by TIGTA and will continue to follow this practice.
- For the yK1 system, the Office of Research is devising an automated e-mail reminder system to alert users that their accounts will be disabled if they do not access them during a 45 day period. The Office of Research will test this new application and deploy it by the end of the year. Upon deployment of the e-mail alert system, the Office of Research will begin disabling accounts that have been unused for 45 days or more.
- RAS will develop and implement a policy of removing accounts on CDW and yK1 that have not been used in more than 90 days.
- For CDW and yK1, all unnecessary generic or shared accounts will be removed or locked. For SOI-DPS, many of these accounts were removed or disabled during the course of the TIGTA audit, and the remainder will be analyzed and removed or locked. All former employee accounts on all three systems have been removed, and a system will be put in place to ensure employees are removed from these systems as they terminate employment.
- RAS has resolved the issue of [REDACTED]
- 3(d) [REDACTED]
- RAS will continue to follow up on identified security weaknesses to ensure that they are corrected in a timely manner. All identified security weaknesses will be tracked on the Plan of Action & Milestones (POA&M) for the system, and that POA&M will be kept in the Trusted Agent FISMA (TAF) program.

IMPLEMENTATION DATE

January 15, 2009

RESPONSIBLE OFFICIAL

Security Officer, Research, Analysis, and Statistics



*The Office of Research, Analysis, and Statistics Needs to
Address Computer Security Weaknesses*



DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

CORRECTIVE ACTION MONITORING PLAN

Monitoring will be conducted as part of the regular reporting within the organization.

RECOMMENDATION 3

Coordinate with the Modernization and Information Technology Services organization to:

- Implement secure methods of transferring sensitive data between computers.
- Ensure that scanning software is used to periodically scan the RAS organization's systems for security weaknesses.

CORRECTIVE ACTION

- Based on Plan of Actions & Milestones (POA&Ms) and Security Certification & Accreditations, CDW and yK1 have already implemented secure methods of transferring data between our systems using Secure File Transfer Protocol (FTP) and Secure Shell (SSH),
- RAS will coordinate with MITS and the Computer Security Incident Response Center (CSIRC) to ensure scanning software is used to periodically scan the RAS systems for security weaknesses. In addition, MITS/Cybersecurity, including CSIRC, currently performs security assessments of the RAS enterprise systems on a quarterly basis. CSIRC has offered to provide recurring security assessments of the RAS infrastructure, to provide follow-up assessments to ensure remediation of identified vulnerabilities. RAS will work with CSIRC to implement these suggested changes. RAS will coordinate with MITS and CSIRC to ensure scanning software is used to periodically scan the RAS systems for security weaknesses.
- RAS is working with MITS to make sure that files transferred from Martinsburg Computing Center (MCC) are sent securely other than via FTP. However, FTP cannot be disabled on RAS machines until there are other means available for MCC to send data securely to RAS. RAS will coordinate with MITS to find secure methods for data transfer.

IMPLEMENTATION DATE

The RAS employees temporarily assigned IT security duties until the selection of a Security Officer are currently coordinating with MITS to explore new secure methods for data transfer. They are also currently working with MITS to acquire additional software for, or schedule, periodic scanning of RAS systems. Coordination with MITS began August 1, 2008.

RESPONSIBLE OFFICIAL

Security Officer, Research, Analysis, and Statistics



*The Office of Research, Analysis, and Statistics Needs to
Address Computer Security Weaknesses*



DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

CORRECTIVE ACTION MONITORING PLAN

Monitoring will be conducted as part of the regular reporting within the organization.

RECOMMENDATION 4

Remind managers to periodically review Form 5081 records to validate that access to systems is limited to only those who have a need. Managers should also be reminded to verify that potential users have received favorable background investigations before granting them access to systems.

CORRECTIVE ACTION

RAS agrees with this recommendation, and use of Online 5081 records are being used to validate that system access is granted on a need-to-know basis. We will periodically review Form 5081 records for all systems. IRS users will not be granted access without first receiving favorable background clearances. At this time, IRS investigations are taking six months or more for contractors. Since we rely on contractor support to keep CDW running, we will restrict system access and have federal employees closely monitor the work of contractors throughout regular working hours until they have received a favorable background investigation.

In a related matter, TIGTA expressed a concern about staff members of the Joint Committee on Taxation (JCT) who are accessing tax data via the SOI-DPS system. The Congressional JCT staff are statutorily permitted to view tax return data and are not subject to Executive Branch oversight, including background investigations.

IMPLEMENTATION DATE

Completed August 1, 2008; will be managed by the RAS employees temporarily assigned IT security duties until selection of the Security Officer.

RESPONSIBLE OFFICIAL

Security Officer, Research, Analysis, and Statistics, RAS Office Directors

CORRECTIVE ACTION MONITORING PLAN

Monitoring will be conducted as part of the regular reporting within the organization.

RECOMMENDATION 5

Ensure that audit and accountability controls are sufficient by requiring audit logs to be maintained a minimum of 6 years and to be periodically reviewed by the security officer.

CORRECTIVE ACTION

RAS agrees with this recommendation. Audit logs will now be retained for six years, and the security officer designated in Recommendation #1 will perform these reviews.



*The Office of Research, Analysis, and Statistics Needs to
Address Computer Security Weaknesses*



DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

IMPLEMENTATION DATE

Partially implemented. Audit logs are now being retained for six years. The two RAS employees temporarily assigned IT security duties will begin to review the logs on September 1, 2008, until the selection of the Security Officer, who will assume that duty.

RESPONSIBLE OFFICIAL

Security Officer, Research, Analysis, and Statistics

CORRECTIVE ACTION MONITORING PLAN

Monitoring will be conducted as part of the regular reporting within the organization.

RECOMMENDATION 6

Require managers to ensure that offsite storage is used for system and data backup files.

CORRECTIVE ACTION

RAS agrees with this recommendation. Certain RAS sites, in particular SOI sites in Ogden and Covington have been using offsite storage. For several years, backup tapes for other RAS systems were stored in the main IRS building at 1111 Constitution Avenue. After that building flooded, RAS negotiated with MITS to add National Office tapes to the Iron Mountain offsite storage contract, and RAS is now working with Enterprise Operations (EOPS) in this regard to fully implement this recommendation.

IMPLEMENTATION DATE

Fully implemented by December 31, 2008.

RESPONSIBLE OFFICIAL

Director, Office of Research and Director, Statistics of Income

CORRECTIVE ACTION MONITORING PLAN

Monitoring will be conducted as part of the regular reporting within the organization.

RECOMMENDATION 7

Coordinate with the Chief Information Officer to verify that intrusion detection systems are installed on all systems and virus protection software is current.

CORRECTIVE ACTION

RAS is coordinating with MITS/Cybersecurity to install Host Intrusion Detection software (HIDS). Anti-virus software is already being installed on all Windows-based servers and workstations. UNIX servers will have anti-virus software installed once it is available for purchase through MITS channels.



*The Office of Research, Analysis, and Statistics Needs to
Address Computer Security Weaknesses*



DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

IMPLEMENTATION DATE

January 15, 2009.

RESPONSIBLE OFFICIAL

Director, Research, Analysis, and Statistics

CORRECTIVE ACTION MONITORING PLAN

Monitoring will be conducted as part of the regular reporting within the organization.