TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Key Security Controls of the Currency and Banking Retrieval System Have Not Been Implemented

September 2003

Reference Number: 2003-20-211

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.

Phone Number | 202-622-6500
Email Address | TIGTACommunications@tigta.treas.gov
Web Site | http://www.tigta.gov

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

INSPECTOR GENERAL
for TAX
ADMINISTRATION

September 26, 2003

MEMORANDUM FOR COMMISSIONER, SMALL BUSINESS/SELF-EMPLOYED
DIVISION
CHIEF INFORMATION OFFICER

Gordon C. Milbourn III

FROM: Gordon C. Milbourn III
Assistant Inspector General for Audit (Small Business and
Corporate Programs)

SUBJECT: Final Audit Report - Key Security Controls of the Currency and
Banking Retrieval System Have Not Been Implemented
(Audit # 200320004)

This report presents the results of our review of the Currency and Banking Retrieval System (CBRS). The overall objective of this review was to determine whether appropriate security policies and procedures have been developed, effectively implemented, and tested to protect the CBRS from malicious intrusions and unauthorized access.

The CBRS is an online database that contains sensitive information on large cash and suspicious financial transactions reported under the Bank Secrecy Act (BSA).[1] The BSA requires financial institutions, trades or businesses, and other persons to report to the Federal Government a variety of financial transactions, such as bank deposits and withdrawals made in cash exceeding $10,000. Approximately 13 million BSA reports are filed each year. This financial information is used by about 16 Federal Government agencies and over 75 state and local law enforcement agencies for examination, compliance, and enforcement efforts. The sensitivity of the data and the volume of accounts on the CBRS make it an attractive target for persons wanting to steal, manipulate, or destroy the information.

The Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) is one of the key agencies responsible for establishing, overseeing, and implementing

[1] Pub. L. No. 91-508, 84 Stat. 1114 to 1124 (1970) (codified as amended in scattered sections of 12 U.S.C., 15 U.S.C., and 31 U.S.C.)

policies to prevent and detect money laundering. The FinCEN is also responsible for screening and granting access to non-Internal Revenue Service (IRS) users of the CBRS. The IRS Small Business/Self-Employed (SB/SE) Division is the business owner of the CBRS database and is ultimately responsible for the security controls of the CBRS. The Detroit Computing Center is responsible for the design, maintenance, and upgrading of the CBRS.

The IRS has developed adequate security policies and procedures to protect CBRS data. Policies and procedures have been effectively implemented for 6 of the 14 control topics we reviewed. However, management did not implement or test several key IRS policies and procedures pertaining to the other eight control topics. As a result, security of the CBRS is not adequate. Specifically, SB/SE Division management has not:

- Maintained up-to-date risk assessments and security plans.
- Recertified the CBRS after the authority to operate expired in February 2001.
- Devoted sufficient attention to limiting the number of persons with access to the CBRS.
- Ensured background investigations had been performed for those granted access.
- Ensured employees with key security responsibilities have been properly trained.
- Provided sufficient attention to technical access controls and audit trails.

We attribute management's noncompliance with IRS policies and procedures to inadequate concern about the security of the CBRS. We recognize that management must balance security needs with other operational concerns. However, due to the sensitive nature of the data maintained on the CBRS and the wide access given to the data, we believe that management did not give sufficient priority to the security of this system.

To improve security over the CBRS, we recommended actions that should be taken by the Commissioner, SB/SE Division, and the Chief Information Officer. The risk assessment, security plan, and certification should be updated. The practice of reviewing security controls annually needs to be implemented. Operational and technical controls must be improved to limit access to the CBRS to those employees who need it to conduct their jobs. All required information, including background information status, must be included on the authorization form before creating a CBRS user account. All employees with CBRS responsibilities should be provided sufficient training to stay informed of security issues. Management should also ensure that the purpose of any group granted access to the CBRS is well defined and that only those personnel with a need are assigned to a group. In addition, audit trails should be executed routinely to detect inappropriate activities.

Management's Response: The Commissioner, SB/SE Division, and the Chief Information Officer agreed with the recommendations in this report and stated that corrective actions will be taken to assure that CBRS security is adequate. Corrective actions include completing the system certification process; implementing system-based security reviews; implementing a system users archive procedure, including all data download activity on audit trails; and reviewing for completeness all authorizations submitted to create user accounts and rejecting those that are incomplete. Actions will also include issuing a written document to the FinCEN outlining IRS and Department of the Treasury security directives that apply to the CBRS, ensuring that proper training is given to employees with mainframe security responsibilities, better defining access privileges of groups and ensuring that CBRS users are in the proper user groups, and establishing an action plan to create the proper audit trail reports and ensure that they are reviewed. Management's complete response to the draft report is included as Appendix IV.

The Treasury Inspector General for Tax Administration (TIGTA) has designated this report as Limited Official Use (LOU) pursuant to Treasury Directive TD P-71-10, Chapter III, Section 2, "Limited Official Use Information and Other Legends" of the Department of Treasury Security Manual. Because this document has been designated LOU, it may only be made available to those officials who have a need to know the information contained within this report in the performance of their official duties. This report must be safeguarded and protected from unauthorized disclosure; therefore, all requests for disclosure of this report must be referred to the Disclosure Section within the TIGTA's Office of Chief Counsel.

Copies of this report are also being sent to the IRS managers who are 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.

Table of Contents

TD P 15-71

Key Security Controls of the Currency and Banking Retrieval System Have Not Been Implemented

Background

The Currency and Banking Retrieval System (CBRS) contains sensitive information on large cash and suspicious financial transactions reported under the Bank Secrecy Act (BSA).[1] The BSA requires financial institutions, trades or businesses, and other persons to report to the Federal Government a wide variety of financial transactions, such as bank deposits and withdrawals made in cash exceeding $10,000. Each year approximately 13 million BSA reports are filed.

The CBRS is an online database that contains records of over 120 million BSA reports. The reports are kept in the CBRS for 10 years and then archived. The CBRS resides on a mainframe computer at the Internal Revenue Service's (IRS) Detroit Computing Center (DCC).

IRS field agents query the CBRS when performing work in the Examination, Collection, and Criminal Investigation functions. Federal, state, and local law enforcement agencies (e.g., Customs and Border Protection, Department of Justice, Drug Enforcement Administration) may also query the database for researching tax cases, tracking money-laundering activities, obtaining investigative leads, gathering intelligence for tracking currency flows, and corroborating information.

Certain regulatory agencies (e.g., the Federal Reserve System, Securities and Exchange Commission) also use the CBRS for general examination, compliance, and enforcement efforts. About 16 Federal Government agencies and over 75 state and local law enforcement agencies have direct access to the CBRS.

The Department of the Treasury's Financial Crimes Enforcement Network (FinCEN), one of the key agencies responsible for establishing, overseeing, and implementing policies to prevent and detect money laundering, is responsible for screening and granting access to non-IRS users of the CBRS. The IRS Small Business/Self-Employed

[1] Pub. L. No. 91-508, 84 Stat. 1114 to 1124 (1970) (codified as amended in scattered sections of 12 U.S.C., 15 U.S.C., and 31 U.S.C.)

(SB/SE) Division[2] is the business owner of the CBRS and is ultimately responsible under the Federal Information Security Management Act (FISMA)[3] for the security controls of the CBRS. The DCC, a part of the IRS Modernization, Information Technology and Security (MITS) Services organization,[4] is responsible for the design, maintenance, and upgrading of the CBRS.

During this review, we assessed the security of the CBRS database. To accomplish this, we used the *Security Self-Assessment Guide for Information Technology Systems* (Special Publication 800-26) prepared by the National Institute of Standards and Technology (NIST). This document builds on the *Federal Information Technology Security Assessment Framework* developed by the NIST for the Federal Chief Information Officer (CIO) Council.

The NIST Guide addresses 17 security control topics that focus on management, operational, and technical controls. In addition, the Guide provides control objectives and techniques that can be measured for each control topic. To measure the progress of the implementation for the needed security control, the NIST Guide provides five levels of effectiveness for each answer to a security control question:

- Level 1 – control objective is documented in a security policy.
- Level 2 – security controls are documented as procedures.
- Level 3 – procedures have been implemented.
- Level 4 – procedures and security controls are tested and reviewed.

[2] The SB/SE Division serves the needs of businesses with assets of $10 million or less. It provides education, assistance, return processing, and compliance services for these customers.
[3] The FISMA is part of the E-Government Act of 2002, Pub. L. No. 107-347, Title III, Section 301, 2002.
[4] The MITS Services organization meets the information technology needs of the IRS by delivering information technology systems, products, services, and support.

- Level 5 – procedures and security controls are fully integrated into a comprehensive program.

We did not review 3 of the 17 control topics contained in the NIST Guide. The three topics (life cycle, physical security, and incident response capability) either do not apply to operational systems or have been extensively covered in other Treasury Inspector General for Tax Administration (TIGTA) audits.

The audit was performed from January to April 2003 in the DCC and the FinCEN Headquarters in Washington, D.C. The audit was conducted in accordance with *Government Auditing Standards*. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Management Controls Were Not Kept Up to Date

The IRS has developed adequate security policies and procedures to protect CBRS data. However, policies and procedures had not been effectively implemented for 8 of the 14 control topics we reviewed. The SB/SE Division also had not kept management controls up to date and had not implemented two critical operational controls. In addition, MITS Services had not ensured that technical access controls were effective and had not ensured that audit trails were reviewed. As a result, we concluded that security of the CBRS is not adequate.

Management controls are needed to ensure that appropriate security procedures are implemented to reduce the risks associated with a system. Functional managers charged with maintaining the system are responsible for these controls, which consist of four topics applicable to the CBRS: risk management, review of security controls, certification and accreditation, and system security plan.[5]

The SB/SE Division did not follow IRS policies and procedures for these topics. By not complying with the following procedures, management can have little

[5] Controls in a fifth topic – life cycle – were either not applicable or duplicated in other control topics.

confidence that the CBRS security controls are commensurate with the risks inherent in this system.

We attribute the noncompliance to inadequate concern about the security of the CBRS. We recognize that management must balance security needs with other operational concerns. However, due to the sensitive nature of the data maintained on the CBRS and the wide access given to the data, we believe that management did not give CBRS security sufficient priority.

Risk Management – A risk assessment is the process used for identifying threats and vulnerabilities of a system and the potential impact that a loss of information or the capabilities of the system would have on the agency. It is used as a basis for identifying and selecting appropriate and cost-effective measures for reducing or accepting risks.

The IRS is required to conduct risk assessments for its sensitive systems at least every 3 years, and it must review the risk assessments annually. The last CBRS risk assessment was conducted in May 2001, almost 4 years after the previous risk assessment. SB/SE Division management had not reviewed the risk assessment annually, as required, to ensure it was still valid. When risk assessments are delayed, security threats and vulnerabilities might not be identified timely, and additional controls to reduce these threats and vulnerabilities might not be timely devised and implemented.

Review of Security Controls – The FISMA requires that functional managers perform security reviews at least annually for each of the major systems that support their operations. The extent of such reviews can vary depending on risk and the scope of prior reviews. Without periodic reviews and tests, the IRS may not have adequate assurance that security controls are functioning effectively and providing an adequate level of protection.

The CBRS security controls were last reviewed as part of the May 2001 risk assessment. Prior to the 2001 assessment, the last security review was performed in 1997. At the time of our review, SB/SE Division management still had not taken action to address any of the security weaknesses identified in its May 2001 review. In addition, SB/SE Division management had not reviewed the FinCEN's controls for granting access to the CBRS for non-IRS users.

Certification and Accreditation – Certification is a technical evaluation of an information system to determine how well it meets security requirements, including all applicable Federal laws, policies, regulations, and standards. The certification process is the final step leading to system accreditation, which is the written authorization for a system to operate. All major applications and general support systems must be recertified and reaccredited at least every 3 years, or sooner if major system changes affect the security safeguards.

The CBRS' certification and authority to operate expired on February 28, 2001. Significant documentation required to recertify the CBRS was prepared in 2001 but has not yet been approved.

Security Plan – A security plan should provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The plan should delineate responsibilities and expected behavior of all individuals who access the system. The security plan should be reviewed periodically and updated to reflect current conditions and risks.

The last security plan was completed in May 2001, as part of the ongoing certification and accreditation process. However, it has yet to be approved and signed by management.

Recommendations

The Commissioner, SB/SE Division, should:

1. Take immediate steps to review, update, and approve the CBRS risk assessment and security plan and complete the certification process.

Management's Response: All certification documentation has been completed and the Security Services function has issued the Certification memorandum to the Principal Accrediting Authority (PAA) for accreditation. Once the PAA has signed the accreditation memorandum, the process will be completed.

2. Implement the practice of reviewing security controls annually, as required by the FISMA, and include the FinCEN in such reviews.

Management's Response: In July 2003, the SB/SE Division implemented FISMA-based security reviews for Fiscal Year 2003 that are due for completion by late September 2003. These reviews use the NIST *Self-Assessment Guide* and include the CBRS. Also, the FinCEN conducted a 2003 FISMA review of its computer gateway that offers non-Federal entities access to the CBRS.

Two Critical Operational Controls Were Not Effectively Implemented

Operational controls are primarily implemented and executed by people (as opposed to systems). They cover nine control topics, and all are applicable to the CBRS. We did not review two of the topics (physical security and incident response capability) because they have been addressed extensively in other TIGTA reviews.

Policies and procedures were developed for each of the seven topics reviewed. Procedures were effectively implemented in the following five topics: production and input/output controls, contingency planning, hardware and systems software maintenance, data integrity, and documentation.

However, personnel security access controls and computer security training were not effectively implemented. As a result, the risk of unauthorized use and disclosure is unnecessarily high. We attribute these conditions to inadequate attention to security of the CBRS by SB/SE Division management. We believe that management did not give security a sufficient priority based on the sensitivity of the data on the system and the wide access provided.

Personnel Security – Many important issues in computer security involve human users, designers, implementers, and managers. A broad range of security issues relates to how these individuals interact with computers and the access and authorities they need to do their jobs.

We identified the following personnel security weaknesses:

- User accounts were not deleted from the system even though the users might have no longer needed access to accomplish their jobs.
- Downloading of large blocks of CBRS data was not adequately controlled.
- User accounts were added to the system without evidence of a background investigation having been completed.

User accounts were not deleted when they were no longer needed

At the time of our review, approximately 9,500 user accounts existed on the CBRS database (6,300 IRS employees and 3,200 non-IRS employees). We noted that some accounts had been added to the CBRS as early as 1992. DCC security employees advised us that once a person is added to the CBRS user list, he or she would never be removed.

Employee accounts are automatically disabled for some DCC systems if the accounts are not accessed within 60 days. At the time of our review, using the same 60-day criterion for the CBRS database, approximately 6,600 accounts on the CBRS should have been disabled. The large number of inactive CBRS accounts can result in system administration inefficiencies. In addition, although other controls are in place to limit access to current users, the large number of unnecessary accounts on the CBRS still increases the risk of misuse of the system.

The downloading of large blocks of CBRS data needs to be better controlled

In addition to making individual queries on the CBRS database, users can request programmers to download large blocks of data. Downloads of data present significantly greater risks because of the amounts of data that can be obtained. Further, if a requestor wanted to conceal a request for a certain transaction, a download of many transactions could be requested to prevent a reviewer from identifying the inappropriate query.

We were advised by DCC management that these downloads are completed after the approval of a separate memorandum requesting the data. The requests are reviewed and approved by an Information Technology manager on site at the DCC.

Programmers perform the actual downloading of the data from the CBRS, which violates controls over separation of duties. In addition, downloads are not captured on the audit trail.[6] While the ability to download blocks of data might provide some efficiency to the frequent users of the system, management did not implement basic controls to monitor this process. With the programmers accessing the data directly and audit trail information not recording these transactions, misuse of the data would go undetected.

Users were given access to the CBRS without evidence of required background investigations having been completed

IRS procedures require that employees' backgrounds be investigated before they are given access to sensitive systems. Acknowledgement that the investigations were conducted must be shown on the Information System User Registration/Change Request (Form 5081). IRS managers use Form 5081 to authorize the creation of a user account on systems that employees need to access. The FinCEN is responsible for initiating and processing Forms 5081 for all non-IRS users of the CBRS.

We reviewed 107 Forms 5081 from 3 separate groups of users: 37 IRS employees who work at the DCC, 20 IRS Criminal Investigation function employees who work at several locations, and 50 non-IRS users who were

[6] An audit trail is a series of computer records about an operating system, application, or user activity that establishes what events occurred and who or what caused them.

authorized by the FinCEN. The Forms reviewed were chosen to be representative of the types of system users and by availability at the time of our request.

The Forms 5081 indicated that 85 employees (almost 80 percent of our sample) had been given access to the CBRS without the required background investigation section of the Form having been completed. Specifically, the DDC received 44 of these Forms from the FinCEN and 41 Forms from IRS managers. DCC system administrators added the users to the CBRS without ensuring that the required background information sections of the Forms 5081 had been completed.

Computer Security Training – People are a crucial factor in ensuring the security of computer systems and valuable information resources. Computer security awareness training enhances security by improving awareness of the need to protect system resources. Technical training is particularly essential for computer system staff with key computer security responsibilities. However, there was inadequate emphasis on computer security awareness training provided to non-IRS users of the CBRS and on the continuing professional development of CBRS technical computer staff.

All users of IRS computer systems need to be made aware of their computer security responsibilities and to be held accountable for complying with these responsibilities. To accomplish this, the IRS requires (1) users to review and sign system security rules on the Form 5081 prior to being given system access, (2) users to attend annual computer security awareness refresher training, and (3) managers to certify yearly that their users have received and signed the rules of behavior.

Non-IRS users of the CBRS were not meeting these three requirements. Seven of the 50 Forms 5081 we reviewed that were authorized by the FinCEN did not contain employees' signatures to acknowledge their awareness of the rules. Not having a user's signature could adversely affect future disciplinary action, or even prosecution, should any abuse be discovered. The FinCEN also did not periodically remind non-IRS users of their security responsibilities and did not ensure that users re-signed Forms 5081 each year to acknowledge their awareness of security rules. SB/SE Division management did not provide sufficient oversight of the FinCEN's practices for authorizing access to the CBRS by employees from Federal, state and local agencies.

In addition, technical computer security training was not provided to employees with key security responsibilities. The Federal Information System Controls Audit Manual (issued by the United States General Accounting Office) states that skills of computer staff should be periodically assessed. Agencies should formalize annual training requirements and professional development programs to make certain the skills of technical computer employees are adequate and current. Employee training and professional development should be monitored.

DCC managers did not assess their technical employees' professional development and did not prepare annual training or professional development plans. Additionally, the CBRS computer system staff did not attend continuing education workshops and seminars to enhance the computer security skills that would keep them abreast of recent issues such as new system vulnerabilities, hacker techniques, and mainframe security controls.

Management stated that training funds were not available for this type of training. The risks of theft of data and unauthorized disclosure increase significantly when employees are not able to recognize and protect against new security threats and vulnerabilities.

Recommendations

The Commissioner, SB/SE Division, and CIO should:

3. Establish a logical access control to remove and archive CBRS user accounts when they have not been used for a reasonable time, e.g., 60 days.

Management's Response: The Business Systems Development (BSD) function has implemented a monthly procedure for removing and archiving from the CBRS User Profile accounts that are inactive for 90 days.

4. Establish separation of duties to ensure programmers do not have access to live CBRS data and ensure that audit trails are updated to identify downloads of large blocks of data.

Management's Response: The DCC does not allow computer programmers access to production data (live data) except in special circumstances. The IRS will implement a programming change for audit trail tracking of large blocks of data. Also, batch programs that download/print documents for a special request will require an audit trail subroutine that will contain all necessary information.

5. Remind system administrators that all required information, including background investigation status, must be included on the Form 5081 before creating a CBRS user account.

Management's Response: The IRS has implemented the On-Line 5081 system for all IRS employees and contractors. This system will automatically transfer the background investigation date from the personnel system and insert it into the Form 5081. For non-IRS users, the FinCEN uses paper Forms 5081 to provide background investigation dates. Both the Security Staff and the BSD manager will reject forms submitted by the FinCEN that are incomplete and do not comply with this requirement.

6. Prepare a written document, which would be forwarded to the FinCEN, stipulating the security requirements that the IRS expects the FinCEN to follow. This agreement would help ensure that non-IRS users of the CBRS adhere to the same security standards as IRS employees.

Management's Response: The IRS will issue a written document to the FinCEN regarding security requirements as outlined in the IRS Internal Revenue Manual, the Law Enforcement Manual, and the Department of the Treasury Security Manual.

7. Ensure that DCC site employees with CBRS responsibilities are provided sufficient training to stay abreast of security issues.

Management's Response: Providing security awareness training for specific job functions is being included in Security Services function-sponsored security guidance and training for key staff. This guidance and training includes security responsibilities for mainframe systems, such as the CBRS. The Security Services function will work to ensure that this material will be included in the updated Security Curriculum and made available to all employees with mainframe security responsibilities.

Technical Operating System Controls Were Not Effective and Audit Trails Were Not Reviewed

Technical controls are executed by computer systems. The controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. Three control topics are listed under technical controls, and the IRS has policies and procedures that address all three topics.

Identification and authentication controls were effectively implemented. However, the logical access controls and the audit trails topics had weaknesses. As a result, sensitive CBRS data were at unnecessary risk, and without audit trail information, the IRS would be hindered in investigating potential inappropriate accesses. We attribute these conditions to inadequate attention to security of the CBRS by SB/SE Division management. Again, we believe that management did not give security a sufficient priority based on the sensitivity of the data on the system and the wide access provided.

Logical Access Controls – System-based controls restrict who is to have access to a specific system and the type of transactions and functions that are permitted. IRS policy provides that logical access controls for software programs, databases, data files, and telecommunications access should be based on the principle of "least privilege." That is, users should be granted access to only those information resources they need to perform their official duties. Least privilege limits the risk and damage that can occur because of unauthorized disclosures.

The IRS assigned responsibility for certain transactions to groups of employees. Assigning employees to groups can be an effective and efficient approach for assigning access rights, but it is critical that each employee in the group has a need for all of the access rights provided to the group.

The purpose of groups was not documented, making it difficult for security personnel to determine the appropriate group in which to place a new user. We found that some employees were included in groups although their responsibilities did not require it, resulting in powerful security privileges being given to employees unnecessarily and in separation of duties problems. For example:

- Twenty-five employees could alter or update profiles controlling access to files containing CBRS information, although they did not need this capability to perform their job functions.
- One group consisted of 127 employees (CBRS application programmers, edit and error resolution staff that correct CBRS information, computer operators, and users from the Criminal Investigation function) who had access rights to read, modify, and delete CBRS data. Most programmers do not need to access the CBRS data. Edit and error resolution employees use another application for doing their work. Based on their job responsibilities, many of the other users also did not need this access.
- Three computer support staff members, not assigned to the CBRS, had security administration capabilities allowing them to control access profiles for CBRS files.
- Two application programmers, who had no need to access CBRS data, were included in CBRS user groups with access to these data.
- Two application programmers were assigned administration duties for the mainframe security

system. Three application programmers were assigned administration duties for the CBRS. These duties should be segregated to reduce the opportunities for misuse.

- Management assigned 8 computer staff members to 1 group and 10 to another group that had the most sensitive and powerful privileges over the CBRS database and its security. These privileges need to be restricted to as few employees as possible.

Audit Trails – Audit trails maintain a record of system activity. In conjunction with appropriate tools and procedures, audit trails can provide individual accountability and a means to reconstruct events, detect intrusions, and identify problems. IRS procedures require that audit trails be run and documentation maintained for all sensitive systems.

The DCC did not review audit trail reports for the CBRS application. Management advised us that audit trail reports are produced and reviewed only when a manager has a suspicion that an employee has engaged in inappropriate activity on the system. We found no evidence that audit trail reports had been run for the CBRS.

IRS management has the responsibility for reviewing and analyzing audit trail data. IRS managers have overall responsibility for the security of their systems, applications, and information and should review audit trails on a continuous basis to facilitate the detection of inappropriate and malicious activities and behavior.

By not running and reviewing audit trails, IRS management had no way to identify malicious or inappropriate behavior. The weaknesses found in granting user access to the CBRS makes the review of audit trail data even more critical.

Recommendations

The Commissioner, SB/SE Division, and CIO should:

8. Ensure that the purpose of any group granted access to the CBRS is well defined and that only those personnel with a need are assigned to a group.

Management's Response: The DCC Security Branch has created an Access Matrix for defining those groups that have access to the mainframe computers. It is in the process of perfecting the Matrix. Coordinators will use the perfected Access Matrix for reviews against CBRS groups/users and make corrections as needed.

The CIO should:

9. Ensure that DCC staff members are assigned job responsibilities that do not conflict and that user groups with sensitive and powerful privileges are evaluated to limit membership of those groups to as few computer support staff as possible.

Management's Response: The Access Matrix mentioned above will also be used to limit membership of those groups with sensitive and powerful privileges.

10. Ensure audit trail reports are run and analyzed routinely, not just when requested by an individual manager for a specific purpose.

Management's Response: The SB/SE Division will evaluate the types of audit reports necessary, determine the frequency of the reports to be generated, identify to whom the reports should be sent for review, and submit a Request for Information Services to have the reports created.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether appropriate security policies and procedures have been developed, effectively implemented, and tested to protect the Currency and Banking Retrieval System (CBRS) from malicious intrusions and unauthorized access.
To accomplish this objective, we followed the National Institute of Standards and Technology *Security Self-Assessment Guide for Information Technology Systems* (Special Publication 800-26).

I. To evaluate the adequacy of management controls, we reviewed the Internal Revenue Service (IRS) policies and procedures for developing risk assessments, reviewing security controls, certifying and accrediting systems, and developing security plans. To determine whether these policies and procedures had been implemented effectively, we evaluated the most current documents to determine whether they were up to date and whether actions had been taken to correct prior security findings.

II. To evaluate the adequacy of operational controls, we reviewed the IRS policies and procedures for personnel security, production controls, contingency planning, maintenance, data integrity, documentation, and security training. We visited the Detroit Computing Center (DCC) and the Department of the Treasury Financial Crimes Enforcement Network (FinCEN) in Washington, D.C., and reviewed available documentation and interviewed key employees to determine whether policies and procedures had been implemented effectively. The review of these controls included an examination of 107 Information System User Registration/Change Requests (Form 5081) granting access to the CBRS. Using a judgmental sample, we reviewed the Forms 5081 available for DCC employees (37) and Criminal Investigation function employees (20), and 50 of the available Forms 5081 for non-IRS users authorized by the FinCEN.

III. To evaluate the adequacy of technical controls, we reviewed the IRS policies and procedures for identifying and authenticating users accessing the CBRS, implementing logical controls, and running and reviewing audit trails. To determine whether these policies and procedures had been implemented effectively, we used scanning software to identify security weaknesses, reviewed available documentation, and interviewed key security employees.

Appendix II

Major Contributors to This Report

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)
Steve Mullins, Director
Gerald Horn, Audit Manager
Richard Borst, Senior Auditor
Tom Nacinovich, Senior Auditor
Midori Ohno, Senior Auditor
William Simmons, Auditor

Appendix III

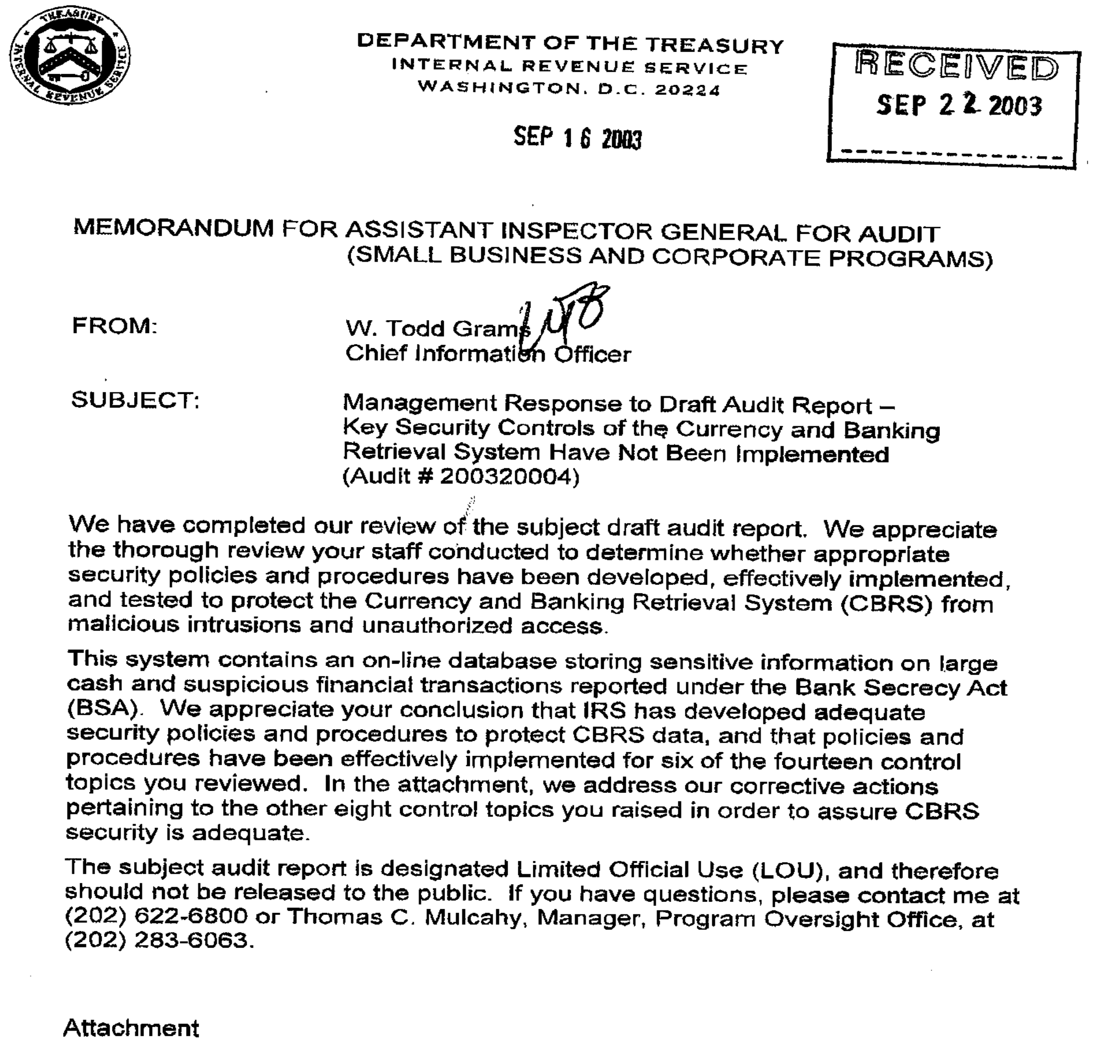
Report Distribution List

Commissioner C
Deputy Commissioner for Operations Support OS
Deputy Commissioner for Services and Enforcement SE
Chief, Information Technology Services OS:CIO:I
Chief, Security Services OS:CIO:S
Director, Compliance, Small Business/Self-Employed Division SE:S:C
Acting Director, Portfolio Management OS:CIO:R:PM
Deputy Director, Planning and Reporting, Security Services OS:CIO:S:S
Director, Detroit Computing Center OS:CIO:I:EO:DC
Deputy Chief Financial Officer, Department of the Treasury

Appendix IV

Management's Response to the Draft Report

TD P 15-71



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

SEP 16 2003

MEMORANDUM FOR ASSISTANT INSPECTOR GENERAL FOR AUDIT
(SMALL BUSINESS AND CORPORATE PROGRAMS)

FROM: W. Todd Grams
Chief Information Officer

SUBJECT: Management Response to Draft Audit Report – Key Security Controls of the Currency and Banking Retrieval System Have Not Been Implemented (Audit # 200320004)

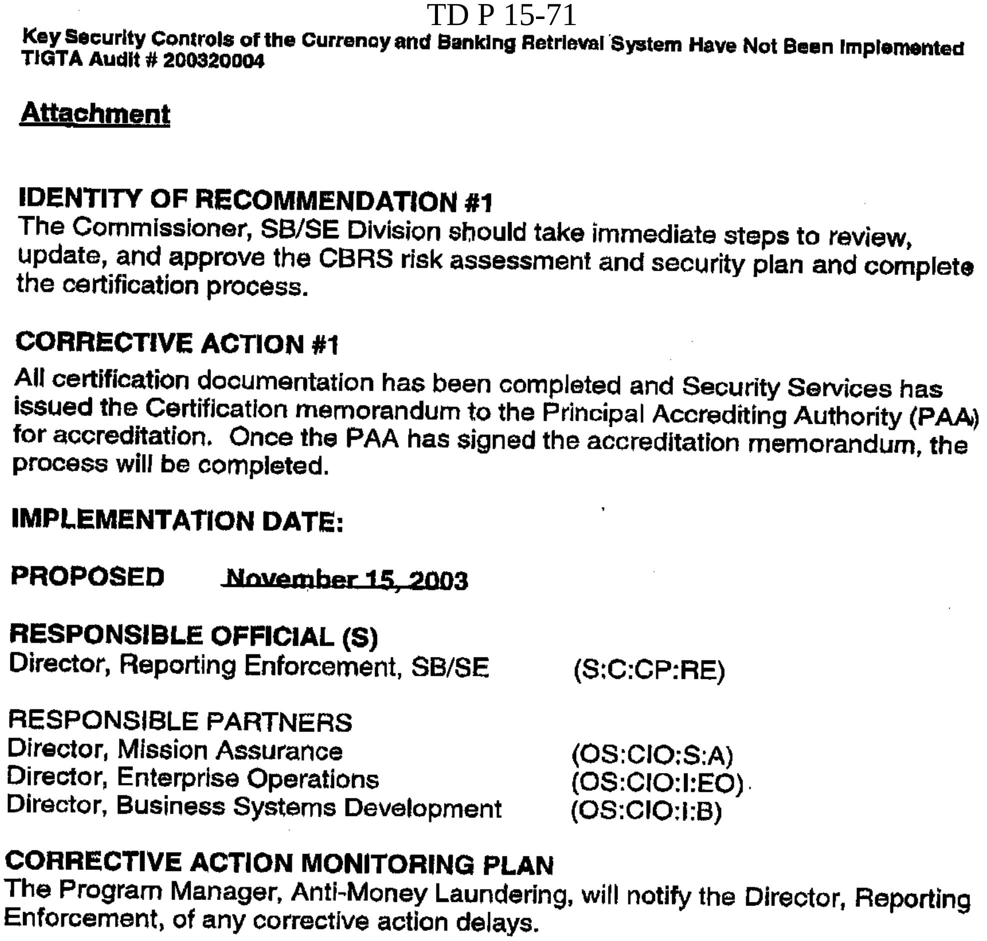
We have completed our review of the subject draft audit report. We appreciate the thorough review your staff conducted to determine whether appropriate security policies and procedures have been developed, effectively implemented, and tested to protect the Currency and Banking Retrieval System (CBRS) from malicious intrusions and unauthorized access.

This system contains an on-line database storing sensitive information on large cash and suspicious financial transactions reported under the Bank Secrecy Act (BSA). We appreciate your conclusion that IRS has developed adequate security policies and procedures to protect CBRS data, and that policies and procedures have been effectively implemented for six of the fourteen control topics you reviewed. In the attachment, we address our corrective actions pertaining to the other eight control topics you raised in order to assure CBRS security is adequate.

The subject audit report is designated Limited Official Use (LOU), and therefore should not be released to the public. If you have questions, please contact me at (202) 622-6800 or Thomas C. Mulcahy, Manager, Program Oversight Office, at (202) 283-6063.

Attachment

TD P 15-71



Key Security Controls of the Currency and Banking Retrieval System Have Not Been Implemented
TIGTA Audit # 200320004

Attachment

IDENTITY OF RECOMMENDATION #1
The Commissioner, SB/SE Division should take immediate steps to review, update, and approve the CBRS risk assessment and security plan and complete the certification process.

CORRECTIVE ACTION #1
All certification documentation has been completed and Security Services has issued the Certification memorandum to the Principal Accrediting Authority (PAA) for accreditation. Once the PAA has signed the accreditation memorandum, the process will be completed.

IMPLEMENTATION DATE:

PROPOSED November 15, 2003

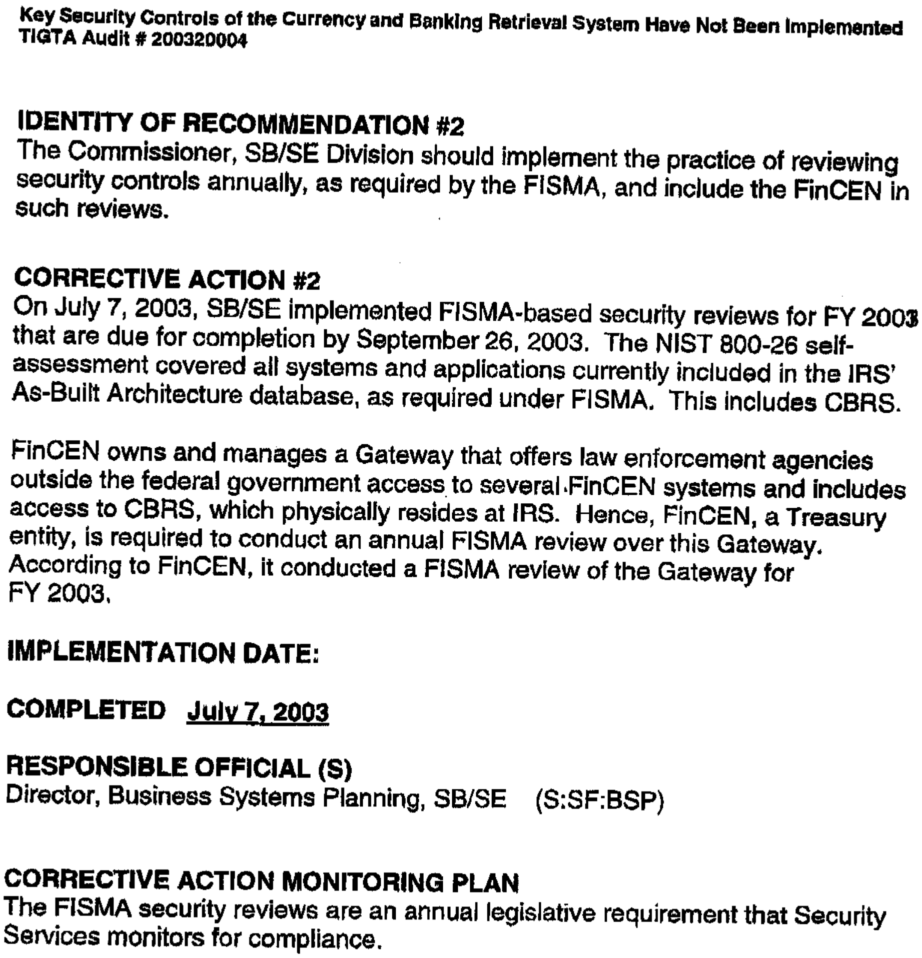
RESPONSIBLE OFFICIAL (S)

Director, Reporting Enforcement, SB/SE	(S:C:CP:RE)

RESPONSIBLE PARTNERS

Director, Mission Assurance	(OS:CIO:S:A)
Director, Enterprise Operations	(OS:CIO:I:EO)
Director, Business Systems Development	(OS:CIO:I:B)

CORRECTIVE ACTION MONITORING PLAN
The Program Manager, Anti-Money Laundering, will notify the Director, Reporting Enforcement, of any corrective action delays.



Key Security Controls of the Currency and Banking Retrieval System Have Not Been Implemented
TIGTA Audit # 200320004

IDENTITY OF RECOMMENDATION #2
The Commissioner, SB/SE Division should implement the practice of reviewing security controls annually, as required by the FISMA, and include the FinCEN in such reviews.

CORRECTIVE ACTION #2
On July 7, 2003, SB/SE implemented FISMA-based security reviews for FY 2003 that are due for completion by September 26, 2003. The NIST 800-26 self-assessment covered all systems and applications currently included in the IRS' As-Built Architecture database, as required under FISMA. This includes CBRS.

FinCEN owns and manages a Gateway that offers law enforcement agencies outside the federal government access to several FinCEN systems and includes access to CBRS, which physically resides at IRS. Hence, FinCEN, a Treasury entity, is required to conduct an annual FISMA review over this Gateway. According to FinCEN, it conducted a FISMA review of the Gateway for FY 2003.

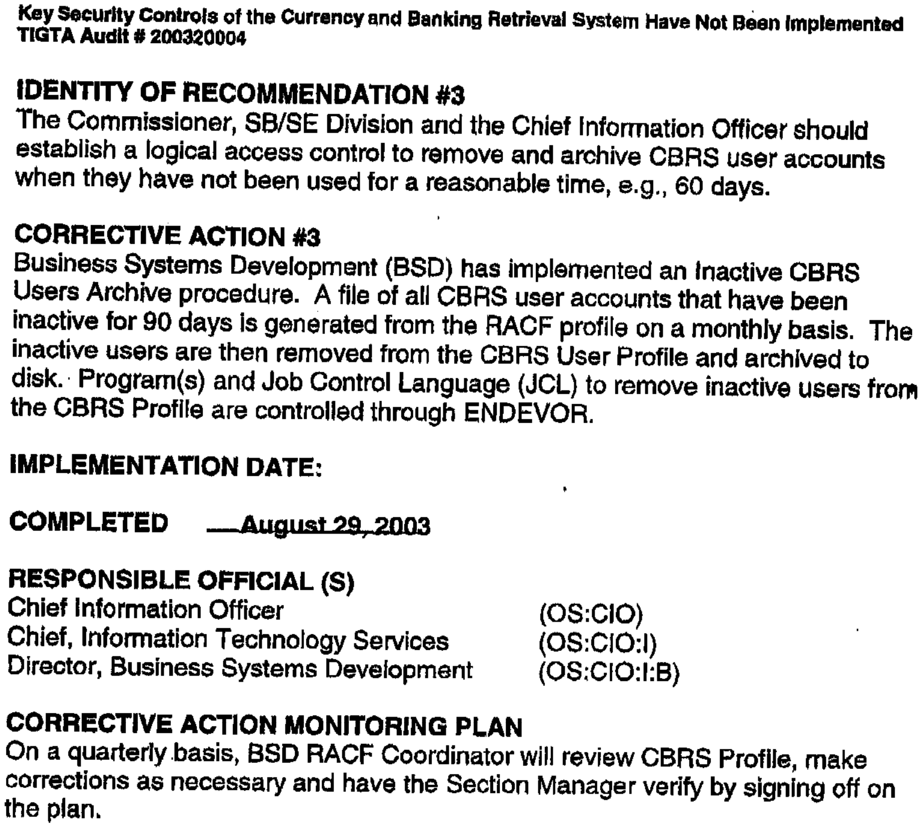
IMPLEMENTATION DATE:

COMPLETED **July 7, 2003**

RESPONSIBLE OFFICIAL (S)
Director, Business Systems Planning, SB/SE (S:SF:BSP)

CORRECTIVE ACTION MONITORING PLAN
The FISMA security reviews are an annual legislative requirement that Security Services monitors for compliance.

TD P 15-71



Key Security Controls of the Currency and Banking Retrieval System Have Not Been Implemented
TIGTA Audit # 200320004

IDENTITY OF RECOMMENDATION #3
The Commissioner, SB/SE Division and the Chief Information Officer should establish a logical access control to remove and archive CBRS user accounts when they have not been used for a reasonable time, e.g., 60 days.

CORRECTIVE ACTION #3
Business Systems Development (BSD) has implemented an Inactive CBRS Users Archive procedure. A file of all CBRS user accounts that have been inactive for 90 days is generated from the RACF profile on a monthly basis. The inactive users are then removed from the CBRS User Profile and archived to disk. Program(s) and Job Control Language (JCL) to remove inactive users from the CBRS Profile are controlled through ENDEVOR.

IMPLEMENTATION DATE:

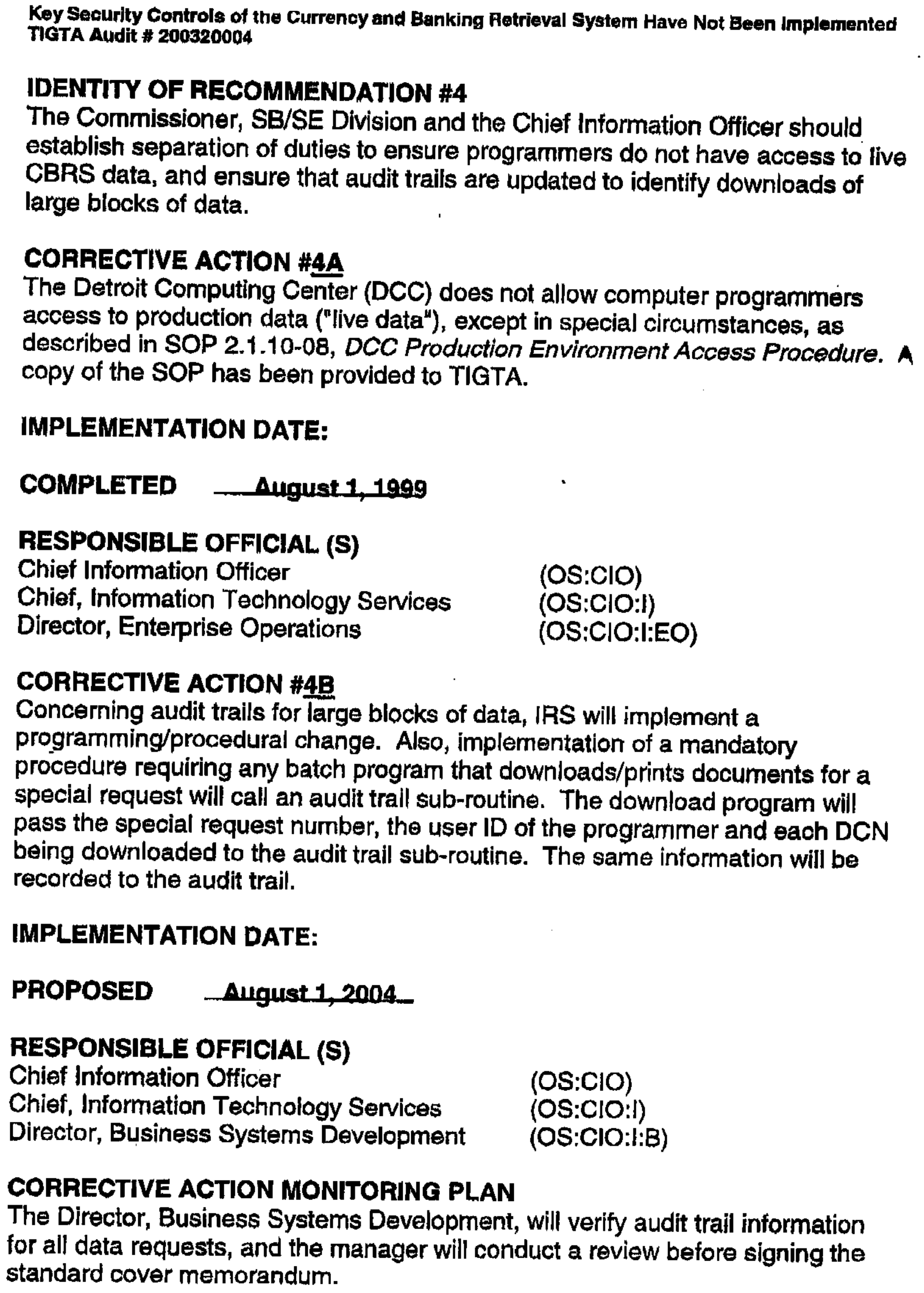
COMPLETED __August 29, 2003__

RESPONSIBLE OFFICIAL (S)

Chief Information Officer	(OS:CIO)
Chief, Information Technology Services	(OS:CIO:I)
Director, Business Systems Development	(OS:CIO:I:B)

CORRECTIVE ACTION MONITORING PLAN
On a quarterly basis, BSD RACF Coordinator will review CBRS Profile, make corrections as necessary and have the Section Manager verify by signing off on the plan.

TD P 15-71



Key Security Controls of the Currency and Banking Retrieval System Have Not Been Implemented
TIGTA Audit # 200320004

IDENTITY OF RECOMMENDATION #4
The Commissioner, SB/SE Division and the Chief Information Officer should establish separation of duties to ensure programmers do not have access to live CBRS data, and ensure that audit trails are updated to identify downloads of large blocks of data.

CORRECTIVE ACTION #4A
The Detroit Computing Center (DCC) does not allow computer programmers access to production data ("live data"), except in special circumstances, as described in SOP 2.1.10-08, *DCC Production Environment Access Procedure.* A copy of the SOP has been provided to TIGTA.

IMPLEMENTATION DATE:

COMPLETED **August 1, 1999**

RESPONSIBLE OFFICIAL (S)

Chief Information Officer	(OS:CIO)
Chief, Information Technology Services	(OS:CIO:I)
Director, Enterprise Operations	(OS:CIO:I:EO)

CORRECTIVE ACTION #4B
Concerning audit trails for large blocks of data, IRS will implement a programming/procedural change. Also, implementation of a mandatory procedure requiring any batch program that downloads/prints documents for a special request will call an audit trail sub-routine. The download program will pass the special request number, the user ID of the programmer and each DCN being downloaded to the audit trail sub-routine. The same information will be recorded to the audit trail.

IMPLEMENTATION DATE:

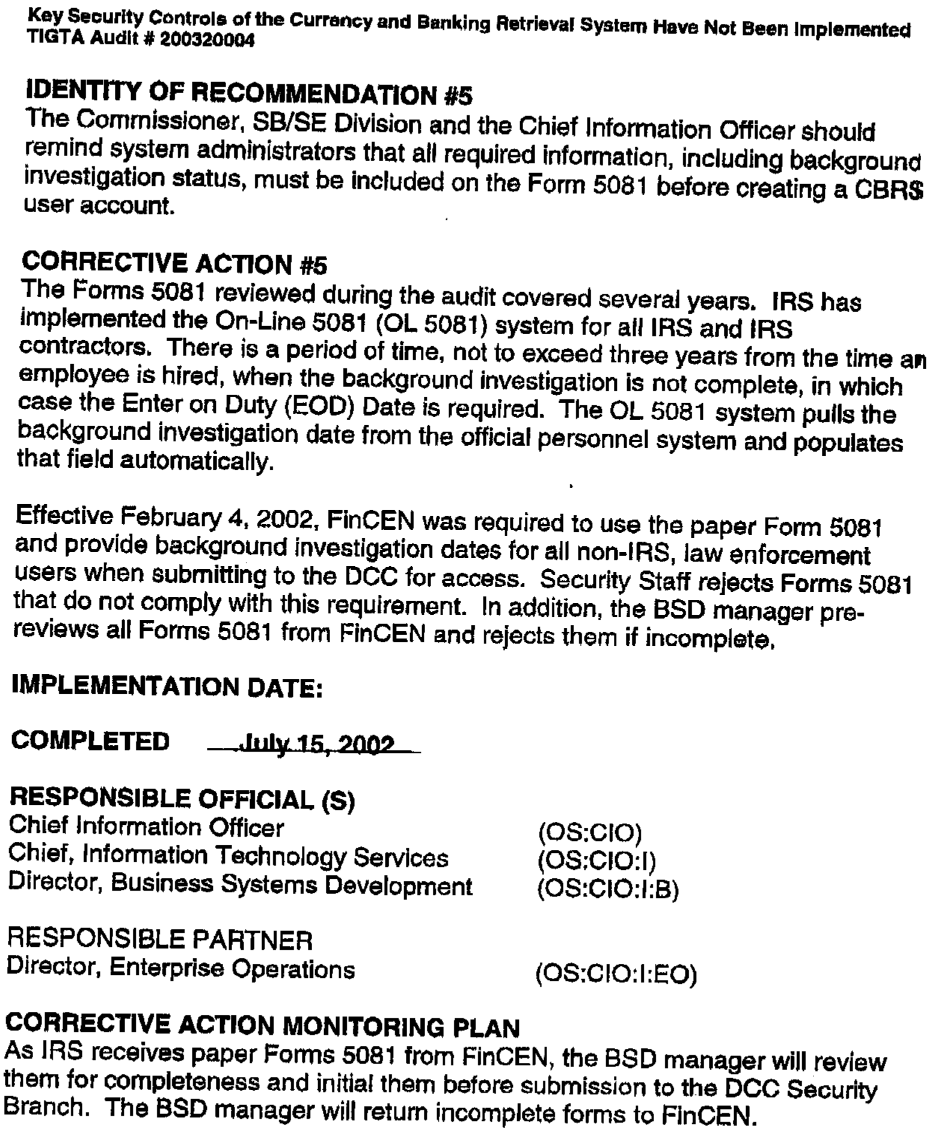
PROPOSED **August 1, 2004**

RESPONSIBLE OFFICIAL (S)

Chief Information Officer	(OS:CIO)
Chief, Information Technology Services	(OS:CIO:I)
Director, Business Systems Development	(OS:CIO:I:B)

CORRECTIVE ACTION MONITORING PLAN
The Director, Business Systems Development, will verify audit trail information for all data requests, and the manager will conduct a review before signing the standard cover memorandum.

TD P 15-71



Key Security Controls of the Currency and Banking Retrieval System Have Not Been Implemented
TIGTA Audit # 200320004

IDENTITY OF RECOMMENDATION #5
The Commissioner, SB/SE Division and the Chief Information Officer should remind system administrators that all required information, including background investigation status, must be included on the Form 5081 before creating a CBRS user account.

CORRECTIVE ACTION #5
The Forms 5081 reviewed during the audit covered several years. IRS has implemented the On-Line 5081 (OL 5081) system for all IRS and IRS contractors. There is a period of time, not to exceed three years from the time an employee is hired, when the background investigation is not complete, in which case the Enter on Duty (EOD) Date is required. The OL 5081 system pulls the background investigation date from the official personnel system and populates that field automatically.

Effective February 4, 2002, FinCEN was required to use the paper Form 5081 and provide background investigation dates for all non-IRS, law enforcement users when submitting to the DCC for access. Security Staff rejects Forms 5081 that do not comply with this requirement. In addition, the BSD manager pre-reviews all Forms 5081 from FinCEN and rejects them if incomplete.

IMPLEMENTATION DATE:

COMPLETED July 15, 2002

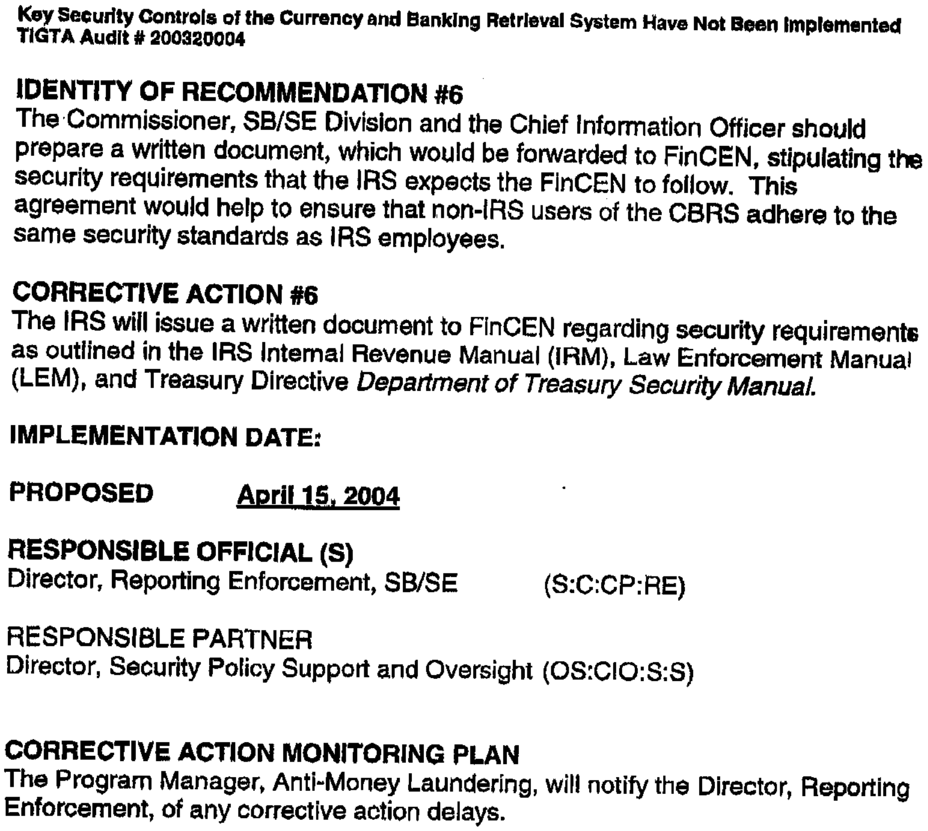
RESPONSIBLE OFFICIAL (S)

Chief Information Officer	(OS:CIO)
Chief, Information Technology Services	(OS:CIO:I)
Director, Business Systems Development	(OS:CIO:I:B)

RESPONSIBLE PARTNER

Director, Enterprise Operations	(OS:CIO:I:EO)

CORRECTIVE ACTION MONITORING PLAN
As IRS receives paper Forms 5081 from FinCEN, the BSD manager will review them for completeness and initial them before submission to the DCC Security Branch. The BSD manager will return incomplete forms to FinCEN.



Key Security Controls of the Currency and Banking Retrieval System Have Not Been Implemented
TIGTA Audit # 200320004

IDENTITY OF RECOMMENDATION #6
The Commissioner, SB/SE Division and the Chief Information Officer should prepare a written document, which would be forwarded to FinCEN, stipulating the security requirements that the IRS expects the FinCEN to follow. This agreement would help to ensure that non-IRS users of the CBRS adhere to the same security standards as IRS employees.

CORRECTIVE ACTION #6
The IRS will issue a written document to FinCEN regarding security requirements as outlined in the IRS Internal Revenue Manual (IRM), Law Enforcement Manual (LEM), and Treasury Directive *Department of Treasury Security Manual.*

IMPLEMENTATION DATE:

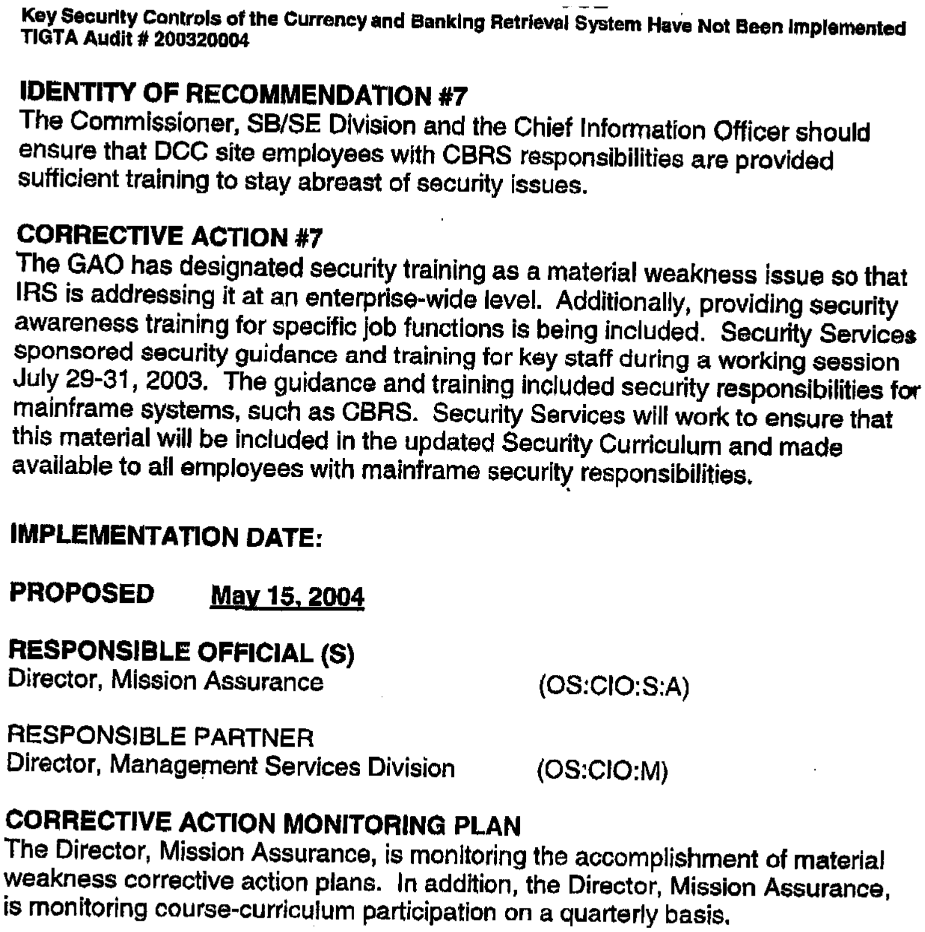
PROPOSED **April 15, 2004**

RESPONSIBLE OFFICIAL (S)
Director, Reporting Enforcement, SB/SE (S:C:CP:RE)

RESPONSIBLE PARTNER
Director, Security Policy Support and Oversight (OS:CIO:S:S)

CORRECTIVE ACTION MONITORING PLAN
The Program Manager, Anti-Money Laundering, will notify the Director, Reporting Enforcement, of any corrective action delays.

TD P 15-71



Key Security Controls of the Currency and Banking Retrieval System Have Not Been Implemented
TIGTA Audit # 200320004

IDENTITY OF RECOMMENDATION #7
The Commissioner, SB/SE Division and the Chief Information Officer should ensure that DCC site employees with CBRS responsibilities are provided sufficient training to stay abreast of security issues.

CORRECTIVE ACTION #7
The GAO has designated security training as a material weakness issue so that IRS is addressing it at an enterprise-wide level. Additionally, providing security awareness training for specific job functions is being included. Security Services sponsored security guidance and training for key staff during a working session July 29-31, 2003. The guidance and training included security responsibilities for mainframe systems, such as CBRS. Security Services will work to ensure that this material will be included in the updated Security Curriculum and made available to all employees with mainframe security responsibilities.

IMPLEMENTATION DATE:

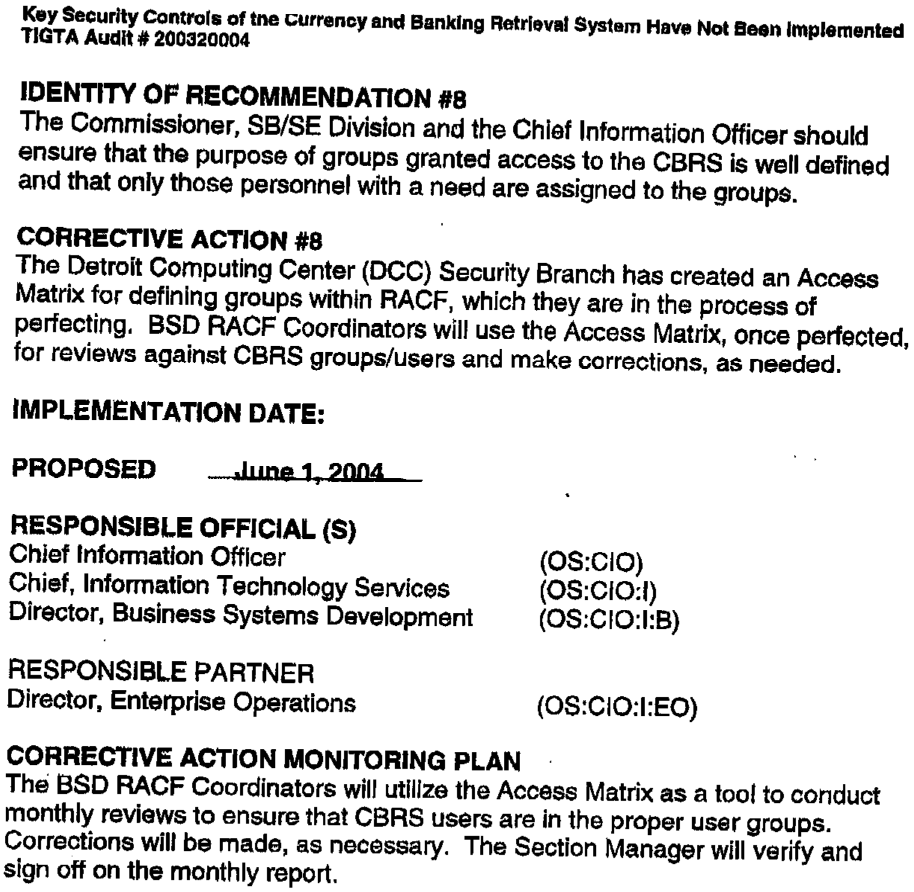
PROPOSED **May 15, 2004**

RESPONSIBLE OFFICIAL (S)
Director, Mission Assurance (OS:CIO:S:A)

RESPONSIBLE PARTNER
Director, Management Services Division (OS:CIO:M)

CORRECTIVE ACTION MONITORING PLAN
The Director, Mission Assurance, is monitoring the accomplishment of material weakness corrective action plans. In addition, the Director, Mission Assurance, is monitoring course-curriculum participation on a quarterly basis.

TD P 15-71



Key Security Controls of the Currency and Banking Retrieval System Have Not Been Implemented
TIGTA Audit # 200320004

IDENTITY OF RECOMMENDATION #8
The Commissioner, SB/SE Division and the Chief Information Officer should ensure that the purpose of groups granted access to the CBRS is well defined and that only those personnel with a need are assigned to the groups.

CORRECTIVE ACTION #8
The Detroit Computing Center (DCC) Security Branch has created an Access Matrix for defining groups within RACF, which they are in the process of perfecting. BSD RACF Coordinators will use the Access Matrix, once perfected, for reviews against CBRS groups/users and make corrections, as needed.

IMPLEMENTATION DATE:

PROPOSED June 1, 2004

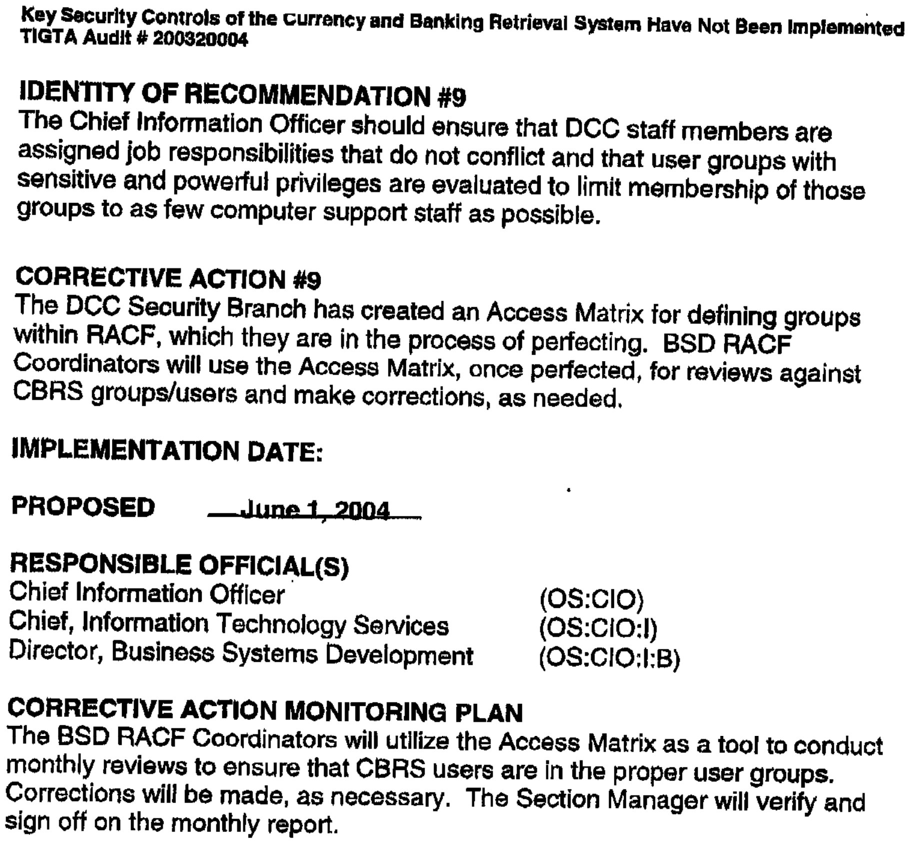
RESPONSIBLE OFFICIAL (S)

Chief Information Officer	(OS:CIO)
Chief, Information Technology Services	(OS:CIO:I)
Director, Business Systems Development	(OS:CIO:I:B)

RESPONSIBLE PARTNER

Director, Enterprise Operations	(OS:CIO:I:EO)

CORRECTIVE ACTION MONITORING PLAN
The BSD RACF Coordinators will utilize the Access Matrix as a tool to conduct monthly reviews to ensure that CBRS users are in the proper user groups. Corrections will be made, as necessary. The Section Manager will verify and sign off on the monthly report.



Key Security Controls of the Currency and Banking Retrieval System Have Not Been Implemented
TIGTA Audit # 200320004

IDENTITY OF RECOMMENDATION #9

The Chief Information Officer should ensure that DCC staff members are assigned job responsibilities that do not conflict and that user groups with sensitive and powerful privileges are evaluated to limit membership of those groups to as few computer support staff as possible.

CORRECTIVE ACTION #9

The DCC Security Branch has created an Access Matrix for defining groups within RACF, which they are in the process of perfecting. BSD RACF Coordinators will use the Access Matrix, once perfected, for reviews against CBRS groups/users and make corrections, as needed.

IMPLEMENTATION DATE:

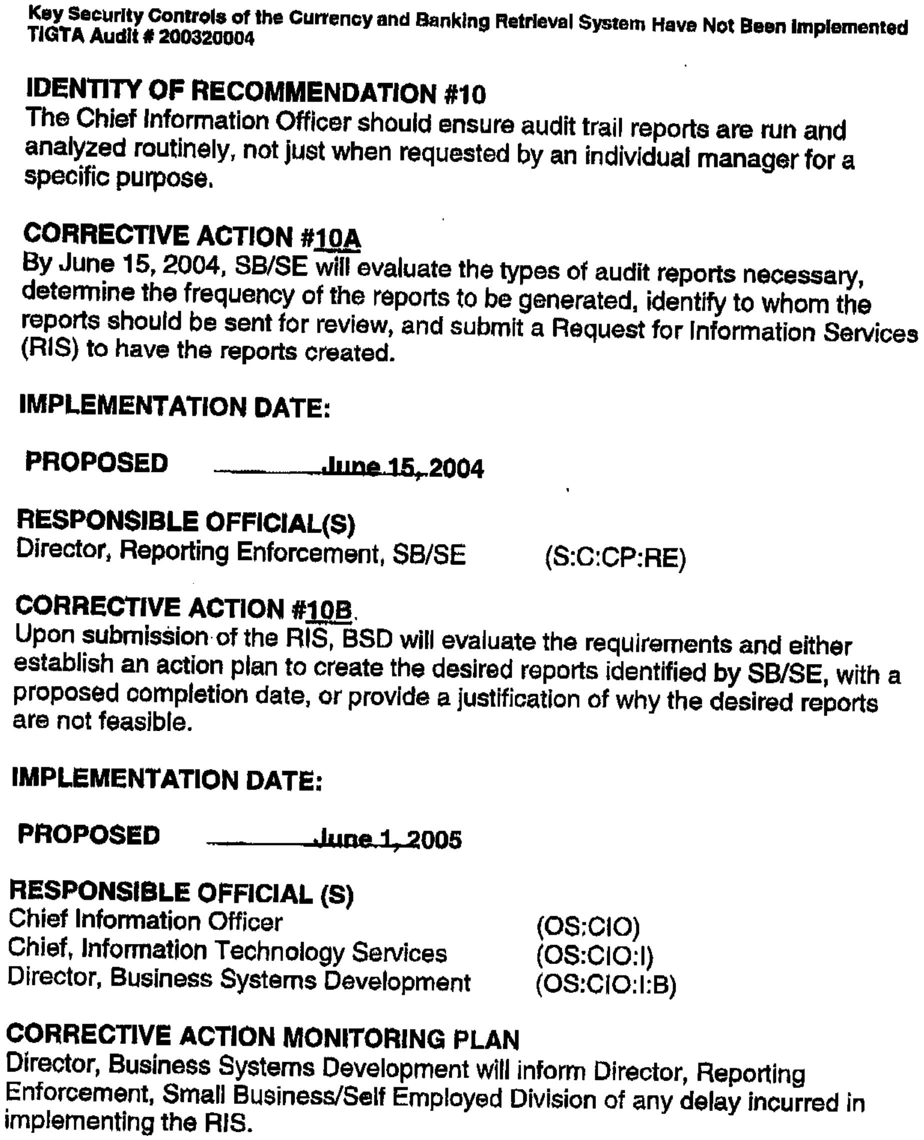
PROPOSED June 1, 2004

RESPONSIBLE OFFICIAL(S)

Chief Information Officer	(OS:CIO)
Chief, Information Technology Services	(OS:CIO:I)
Director, Business Systems Development	(OS:CIO:I:B)

CORRECTIVE ACTION MONITORING PLAN

The BSD RACF Coordinators will utilize the Access Matrix as a tool to conduct monthly reviews to ensure that CBRS users are in the proper user groups. Corrections will be made, as necessary. The Section Manager will verify and sign off on the monthly report.



Key Security Controls of the Currency and Banking Retrieval System Have Not Been Implemented
TIGTA Audit # 200320004

IDENTITY OF RECOMMENDATION #10
The Chief Information Officer should ensure audit trail reports are run and analyzed routinely, not just when requested by an individual manager for a specific purpose.

CORRECTIVE ACTION #10A
By June 15, 2004, SB/SE will evaluate the types of audit reports necessary, determine the frequency of the reports to be generated, identify to whom the reports should be sent for review, and submit a Request for Information Services (RIS) to have the reports created.

IMPLEMENTATION DATE:

PROPOSED June 15, 2004

RESPONSIBLE OFFICIAL(S)
Director, Reporting Enforcement, SB/SE (S:C:CP:RE)

CORRECTIVE ACTION #10B
Upon submission of the RIS, BSD will evaluate the requirements and either establish an action plan to create the desired reports identified by SB/SE, with a proposed completion date, or provide a justification of why the desired reports are not feasible.

IMPLEMENTATION DATE:

PROPOSED June 1, 2005

RESPONSIBLE OFFICIAL (S)

Chief Information Officer	(OS:CIO)
Chief, Information Technology Services	(OS:CIO:I)
Director, Business Systems Development	(OS:CIO:I:B)

CORRECTIVE ACTION MONITORING PLAN
Director, Business Systems Development will inform Director, Reporting Enforcement, Small Business/Self Employed Division of any delay incurred in implementing the RIS.