

TD P 15-71

**Key Security Controls of the Criminal
Investigation Management Information
System Have Not Been Implemented**

March 2004

Reference Number: 2004-20-081

TD P 15-71



DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

INSPECTOR GENERAL
for TAX
ADMINISTRATION

March 30, 2004

MEMORANDUM FOR CHIEF, CRIMINAL INVESTIGATION

Gordon C. Milbourn III

FROM: Gordon C. Milbourn III
Acting Deputy Inspector General for Audit

SUBJECT: Final Audit Report - Key Security Controls of the Criminal Investigation Management Information System Have Not Been Implemented (Audit # 200320012)

This report presents the results of our review of the security controls of the Criminal Investigation Management Information System (CIMIS). 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 CIMIS from malicious intrusions and unauthorized access.

The CIMIS processes sensitive information including personnel and investigative data. It tracks the status and progress of criminal investigations and the time expended by special agents. It also provides the basis for decisions regarding disposition of cases at both the local and national levels.

In summary, the Internal Revenue Service (IRS) has developed adequate security policies and procedures to protect the CIMIS data. Policies and procedures have been effectively implemented for 4 of the 14 control topics we reviewed. However, management did not implement or test several key IRS policies and procedures pertaining to the other 10 control topics. As a result, security of the CIMIS is not adequate. For example, Criminal Investigation (CI) function management has not:

- Maintained up-to-date risk assessments and security plans.
- Tested the technical contingency plan for the CIMIS.
- Kept servers and workstations up to date with the latest security patches.
- Provided sufficient attention to technical controls and audit trails.

TD P 15-71

Management's noncompliance with IRS policies and procedures demonstrates that insufficient attention is being given to the security of the CIMIS. We recognize that management must balance security controls with other operational concerns. However, due to the sensitive nature of the data maintained on the CIMIS and the wide access given to the data, the security controls for the CIMIS are not adequate.

The CIMIS is somewhat unique compared with most other IRS systems because it resides on the CI function's network. The Office of the Chief, Mission Assurance, is responsible for maintaining most IRS networks; however, the CI function's network is maintained by CI's own system administrators and security employees and is not subject to the enterprise solutions in the same way as the vast majority of IRS systems. The CIMIS application is running on outdated workstations and servers that, in many cases, do not comply with the IRS Common Operating Environment standards. The CI function has plans to upgrade its network operating system. If implemented correctly, the new operating system could eliminate some of the conditions we noted.

To improve security over the CIMIS, we recommended the Chief, CI, submit updated risk assessment and security plans and the results of our review to the Chief, Mission Assurance, so the current certification can be reevaluated. The Chief, CI, should implement the practice of reviewing security controls annually and improve operational controls to limit access to the CIMIS to those employees who need it to conduct their jobs. The Chief, CI, should also ensure contingency plans are tested, all servers and workstations have the latest security patches, operating system controls conform to the rest of the IRS architecture, and audit trails are run and reviewed routinely to detect inappropriate activities.

Management's Response: The Chief, CI, agreed with our recommendations but stated that some security standards may be difficult to meet because the CIMIS, as noted in this report, is housed on older, outdated equipment. The target date for upgrading the CIMIS is April 2005. In the interim, the CI function will take all steps necessary to ensure the security of the system and the data it contains.

Corrective actions will be taken to review the CIMIS risk assessment and security plans to make any updates and changes as required. Management does not believe reevaluating the certification of the CIMIS should be necessary, considering it may only have a lifespan of approximately a year before being upgraded.

The CI function will also implement and monitor procedures to perform annual system security self-assessments. IRS procedures will be implemented to control system access, annual testing of contingency plans will be emphasized, and patch management will be strengthened. Operating systems and controls have been strengthened on CIMIS workstations since our review. Also, procedures have been implemented to accomplish the review of audit trails. Management's complete response to the draft report is included as Appendix IV.

Office of Audit Comment: If the planned upgrade of the CIMIS is operational by April 2005, as scheduled, then we agree with management's reasoning that

reevaluating the certification of the CIMIS should not be necessary. However, if the target date for the system upgrade extends beyond April 2005, we believe the current certification should be reevaluated.

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 the 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.

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.

Key Security Controls of the Criminal Investigation Management Information System Have Not Been Implemented

Table of Contents

Background Page 1

Management Controls Are Not Kept Current..... Page 2

Recommendation 1: Page 5

Recommendation 2: Page 6

Four Critical Operational Controls Were Not Effectively Implemented Page 6

Recommendations 3 through 5: Page 9

Technical Operating System Controls Are Not Adequate and Audit Trails Are Not Reviewed Page 9

Recommendations 6 and 7: Page 12

Appendix I – Detailed Objective, Scope, and Methodology..... Page 14

Appendix II – Major Contributors to This Report Page 15

Appendix III – Report Distribution List..... Page 16

Appendix IV – Management’s Response to the Draft Report..... Page 17

Key Security Controls of the Criminal Investigation Management Information System Have Not Been Implemented

Background

The Criminal Investigation Management Information System (CIMIS) tracks the status and progress of criminal investigations and the time expended by special agents. It is also used as a management tool that provides the basis for decisions regarding disposition of cases at both the local and national levels.

The CIMIS contains extremely sensitive employee and taxpayer information, including Grand Jury information. At the time of our review, approximately 800 Criminal Investigation (CI) function employees were permitted access to the system.

The CIMIS is somewhat unique compared with most other Internal Revenue Service (IRS) systems because it resides on the CI function's network. While the Office of the Chief, Mission Assurance, maintains most other IRS networks, the CI function's own system administrators and security employees maintain its network. Consequently, the CI function's network is not subject to the enterprise solutions in the same way as the vast majority of IRS systems.

Federal law and policy state that functional managers are primarily responsible for the security of the information systems they use. The Federal Information Security Management Act (FISMA)¹ requires that agencies review their systems annually. The Office of Management and Budget (OMB) and the Department of the Treasury require agency functional managers to conduct these reviews using the *Security Self-Assessment Guide for Information Technology Systems* (Special Publication 800-26) prepared by the National Institute of Standards and Technology (NIST).

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

¹ The FISMA is part of the E Government Act of 2002, Pub. L. No. 107-347, Title III, Section 301, 2002.

Key Security Controls of the Criminal Investigation Management Information System Have Not Been Implemented

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

During this review, we assessed the security of the CIMIS database using the NIST Guide. We reviewed 14 of the 17 control topics contained in the Guide. The three topics we did not review (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.

This review was performed in the CI function in Washington, D.C., the National Operations Center in Florence, Kentucky, and the Los Angeles and Oakland, California; Miami, Florida; and New York (Manhattan), New York, field offices during the period July through October 2003. The field offices visited covered 32 posts of duty and 187 CIMIS users. 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 Are Not Kept Current

The IRS has developed adequate security policies and procedures to protect the CIMIS data. Policies and procedures have been effectively implemented for 4 of the 14 control topics we reviewed. However, management did not implement or test several key IRS policies and procedures pertaining to the other 10 control topics. As a result, security of the CIMIS is not adequate.

Key Security Controls of the Criminal Investigation Management Information System Have Not Been Implemented

Management controls should help ensure 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: risk management, review of security controls, certification and accreditation, and system security plan.²

CI function management did not adhere to IRS policies and procedures relating to these topics. As a result, management can have little confidence that the CIMIS security controls are commensurate with the risks associated with the system.

Noncompliance with these policies and procedures indicates that sufficient attention has not been given to the security of the CIMIS. We recognize that management must balance security controls with other operational concerns. However, due to the sensitive data maintained on the CIMIS, we believe this application requires a high level of security.

Risk management

A risk assessment is the process used for identifying threats and vulnerabilities of a system and the potential impact 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 CIMIS risk assessment was conducted in April 1999. Since that assessment, there was no evidence to indicate CI function management had reviewed the risk assessment annually to ensure its validity. When risk assessments are not kept current, 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.

² Controls in a fifth topic, life cycle, were either not applicable or duplicated in other control topics.

Key Security Controls of the Criminal Investigation Management Information System Have Not Been 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 the 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 CIMIS security controls were last reviewed as part of the April 1999 risk assessment. At the time of our review, CI function management still had not taken action to address any of the security weaknesses identified in the 1999 review.

Certification and accreditation

The Chief, Mission Assurance, is responsible for certifying the security of the IRS' sensitive systems. 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. All major applications and general support systems must be recertified at least every 3 years, or sooner if major system changes affect the security safeguards.

The CIMIS certification was signed in September 2002. However, the supporting documentation required to certify the CIMIS was prepared in 1999 and had become obsolete. CI function management stated they were not aware of any major system change that would require an update of the certification documentation.

The CI function should have at least tested the controls before coming to that conclusion. Without an updated evaluation of the controls, there is no assurance that an application has adequate security protection against current threats. Based on the less-than-adequate security controls we identified during our audit, we do not believe the CIMIS should have been certified.

Key Security Controls of the Criminal Investigation Management Information System Have Not Been Implemented

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 1999, as part of the certification and accreditation process. However, as of the time of our review, it had yet to be amended and upgraded by management. An outdated security plan provides no assurance that current risks have been identified.

Recommendations

The Chief, CI, should:

1. Take immediate steps to review and update the CIMIS risk assessment and security plans. Once these documents are amended to reflect the current security environment, they should be forwarded along with the results of our review to the Chief, Mission Assurance, to reevaluate the current certification.

Management's Response: The Chief, CI, stated that CI function personnel will review and update the CIMIS risk assessment and security plans as required. Management does not believe reevaluating the CIMIS certification should be necessary, considering that the system may have a lifespan of approximately a year before being upgraded, the review that CI is undertaking, and the focus on the issues our review provided.

Office of Audit Comment: If the planned upgrade of the CIMIS is operational by April 2005, as scheduled, then we agree with management's reasoning that reevaluating the certification of the CIMIS should not be necessary. However, if the target date for the system upgrade extends beyond April 2005, we believe the current certification should be reevaluated.

Key Security Controls of the Criminal Investigation Management Information System Have Not Been Implemented

2. Assess security controls annually by conducting tests in accordance with the NIST Special Publication 800-26, as required by the OMB and the Department of the Treasury.

Management's Response: The CI function will modify its security assessment procedures to specifically follow the NIST Special Publication 800-26 procedures and format. The Director, Office of Strategy, will review these security assessment procedures to ensure this corrective action is met.

Four 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 CIMIS. 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 four topics: production and input/output controls, data integrity (virus protection and intrusion detection), documentation, and security awareness.

However, personnel security access controls, contingency planning, and hardware and systems software maintenance were not effectively implemented. Consequently the risks associated with unauthorized use and disclosure of data are unnecessarily high. Additionally, in the event of an emergency or disruption, it is unlikely that CI management could resume continuity of operations for the CIMIS in an effective and efficient manner.

We attribute these conditions to management's inadequate attention to and emphasis on security controls of the CIMIS.

Personnel security access controls

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

Key Security Controls of the Criminal Investigation Management Information System Have Not Been Implemented

We identified the following personnel security weaknesses.

- The CIMIS application limits management's flexibility in assigning backup responsibilities. The system requires users to be assigned to either one group or the entire field office; it does not provide for limiting users to a subset of user groups. Therefore, any employee assigned backup responsibilities for even one group has access to the entire field office.

In the Manhattan field office, seven staff members responsible for entering CIMIS data were assigned as backups to the primary staff member in other groups. In the Oakland and Miami field offices, 13 staff members were assigned CIMIS data entry responsibilities for a number of groups. In the Los Angeles field office, in an attempt to limit the number of backups, only three individuals performed backup roles.

The risk of misuse could have been reduced without a business impact by limiting the number of backups. In some cases, employees' access privileges were not revoked when their responsibilities no longer required access to the CIMIS. In other cases, we believe management did not consider the security risks of granting backup responsibilities to too many employees.

- User accounts were added to the system without evidence of authorizations. IRS procedures require that managers document employees' levels of access using the Information System User Registration/Change Request (Form 5081). In 2 of the 4 field offices we visited, 28 and 23 CIMIS users, respectively, were added to the system without any documentation. The CI function did not follow its own requirement that users' access authorities be documented and approved on the CIMIS Request User Form. As a result, users may have had access to the system without needing it to complete their job responsibilities.

Contingency planning

Contingency planning involves more than planning for a move offsite after a disaster destroys a facility. It also

Key Security Controls of the Criminal Investigation Management Information System Have Not Been Implemented

addresses how to keep an organization's critical functions operating in the event of a disruption, large or small.

OMB Circular A-130, *Management of Federal Information Resources* (dated February 1996), requires that, prior to a system being given authority to operate, one of the elements that must be in place is a developed and tested contingency plan. The FISMA requires that functional managers review contingency plans, at least annually, as part of their system reviews.

Management certified the CIMIS in 2002 without testing its contingency plan. The technical contingency plan for the CIMIS has not been tested since July 1999. CI function management was reluctant to test the backup plan because the application was running on old, outdated equipment that could cause a major disruption of CI function activities if the contingency plan was tested.

CIMIS data are backed up and stored at an offsite storage facility. No tests had been performed to test the viability of continuing operations using these data. Resuming operations after an emergency would have been difficult because tape media stored at the offsite facility were neither externally labeled nor periodically inventoried until after our review.

The Acting Security Function Officer was not aware of IRS policies that require magnetic media stored at offsite facilities to be labeled and inventoried. Furthermore, the Acting Security Function Officer had never made an inspection of the offsite storage facility housing CIMIS data.

Hardware and system software maintenance

When a vendor discovers security vulnerabilities with a product, it generally provides patches to its customers. The vulnerabilities are usually well publicized and known by hackers, making the timely installation of patches critical.

We identified 34 operating system vulnerabilities on the 32 computers we tested that resulted because system administrators had not installed current security patches.

Key Security Controls of the Criminal Investigation Management Information System Have Not Been Implemented

Hackers, disgruntled employees, and contractors could take advantage of these vulnerabilities to access sensitive data or disrupt computer operations. Inadequate emphasis on security by CI function management contributed to this issue.

Recommendations

The Chief, CI, should:

3. Ensure a Form 5081 is used to create a user account and remind all CIMIS coordinators that all required information, including level of access, must be included on the Form 5081 before creating a CIMIS user account.

Management's Response: The CI function is currently using the Form 5081 along with another form to create CIMIS user accounts. Procedures will be developed to use only the Form 5081 as the vehicle for documenting approval of CIMIS user accounts. Any additional information deemed necessary will be included in the Special Instructions section of the Form 5081.

4. Test the continuity of business operations on an annual basis.

Management's Response: The CI function will continue to emphasize that continuity of operations tests be performed annually and will develop formal testing procedures.

5. Create a patch management process to ensure all applicable patches are identified, tested, and installed timely.

Management's Response: The implementation of Windows XP and the Microsoft Software Update Services tool will enhance the current system and will allow the CI function to put in place a more formal patch management process.

Technical Operating System Controls Are Not Adequate and Audit Trails Are 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

Key Security Controls of the Criminal Investigation Management Information System Have Not Been Implemented

the IRS has policies and procedures to address all three topics.

Control weaknesses existed for each of the three topics. As a result, sensitive CIMIS data were exposed to unnecessary risk, and the IRS would be hindered in investigating potential inappropriate accesses and improper manipulation of data.

To fully evaluate the security of an application, an agency must also review the network operating system controls. The scope of the NIST *Self-Assessment Guide* includes assessments of both operating system and application controls. When applicable, we included both in our review. The next two control topics (Identification/Authentication and Logical Access Controls) address operating system controls.

The CI function has plans to upgrade its network operating system. If implemented correctly, the new operating system may eliminate some of the conditions noted as a result of our review.

Identification/Authentication

Sixteen of the 32 workstations we tested had vulnerabilities that were directly related to password configuration. The main six-character password (which the CI function requires as a minimum) is weaker than the IRS standard. If a hacker attempted to steal a CI function laptop computer, he or she could more easily crack the password using readily available software.

System administrators on two of the servers supporting the CIMIS were routinely logging in directly as system administrators, rather than as users, using a privilege known as "root access." When this procedure is followed, the audit trail will not record the name of the system administrator who entered systems commands. System administrators should have logged on with their personal user account and then switched to the system administrator's account.

In addition, system administrators shared accounts with no specific user name or password for selected administrative functions on the CI function's network and

Key Security Controls of the Criminal Investigation Management Information System Have Not Been Implemented

local servers. CI management was not able to provide a sound business reason why these accounts were available on the network and agreed that accountability through the use of audit trails is lost for any transactions completed using these accounts.

Logical access controls

System-based controls restrict who has access to a specific system and the type of transactions and functions that are permitted. We scanned 28 workstations and 4 servers using the Internet Security Systems scanning tool for evaluating computer configuration against the SysAdmin, Audit, Network, Security (SANS)/Federal Bureau of Investigations (FBI) Top 20³ lists of common system vulnerabilities. We identified 144 vulnerabilities on the 32 computers that had access to the CIMIS application. All 32 computers exhibited at least 1 of these vulnerabilities that could provide hackers with gateways into the CI function's system.

As we mentioned earlier, 34 of the vulnerabilities identified were due to obsolete patches on the computers. Other vulnerabilities were present because the CI function did not use the Common Operating Environment (COE) used elsewhere in the IRS. Other IRS functions have been very effective in reducing the number of security vulnerabilities by using the COE requirements.

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 continuously

³ The SANS Institute was established in 1989 as a research and education organization for the government and private industry security community. The SANS Institute, along with the FBI, periodically announces a list of top 20 computer security vulnerabilities based on security incidents recently reported. The list is known as the SANS/FBI Top 20.

Key Security Controls of the Criminal Investigation Management Information System Have Not Been Implemented

and analyzed routinely and that documentation be maintained for all sensitive systems.

Management did not require the review of audit trail reports for the CIMIS. Management advised us that audit trail reports are produced; however, the CI Security Function Officer was not able to interpret the audit trail logs in their current format. We obtained copies of CIMIS audit trail data and determined the data are presented in clear text and, with the proper training of users, could be reviewed on a regular basis to detect misuse of the system.

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 regular basis to identify inappropriate and malicious activities and behavior.

Recommendations

The Chief, CI, should:

6. Strengthen the CI function's system administration responsibilities and take immediate action to ensure the operating system controls that support the CIMIS application conform to the rest of the IRS architecture.

Management's Response: The CI function is working to strengthen operating system controls for the CIMIS. The upgraded CIMIS will include strengthened operating system controls. The CI function will ensure appropriate audit recommendations will be included in those controls.

7. Ensure audit trail reports are run continuously and analyzed routinely by the Security Function Officer. Software used by other IRS functions can be used. CI function operations staff, CI function management, and the Security Function Officer should review the audit trail reports being implemented by the Chief, Mission Assurance, and implement them for audit trail analysis within the CI function. Close attention should be paid to high-risk activities such as employees signing on with root access.

Key Security Controls of the Criminal Investigation Management Information System Have Not Been Implemented

Management's Response: The CI function is in the process of permanently filling the Security Officer position. The temporary Security Officer has been analyzing audit trail reports since November 2003. The CI function modified direct root access procedures to make audit trails easier to interpret. Adequate audit trails will be maintained and reviewed.

Key Security Controls of the Criminal Investigation Management Information System Have Not Been Implemented

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 Criminal Investigation Management Information System (CIMIS) 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's (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 Criminal Investigation (CI) function in Washington, D.C., the National Operations Center in Florence, Kentucky, and the Los Angeles and Oakland, California; Miami, Florida; and New York (Manhattan), New York, field offices and reviewed available documentation and interviewed key employees to determine whether policies and procedures had been implemented effectively. We selected these audit sites based on the high volume of CIMIS users and the number of posts of duty covered by these field offices. The review of these controls included examining Information System User Registration/Change Requests (Form 5081), which grant access to the CI function's network and the CIMIS.
- III. To evaluate the adequacy of technical controls, we reviewed the IRS' policies and procedures for identifying and authenticating users accessing the CIMIS, 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. We performed scans of 32 computers. We randomly selected seven workstations from each of the four field offices we visited. We scanned all four servers used by the CIMIS located in Florence, Kentucky, and Washington, D.C. We also reviewed available documentation and interviewed key security employees at the Headquarters office and selected audit sites.

Key Security Controls of the Criminal Investigation Management Information System Have Not Been Implemented

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
David Brown, Senior Auditor
Bret Hunter, Senior Auditor
William Lessa, Senior Auditor
Tom Nacinovich, Senior Auditor
William Simmons, Senior Auditor

**Key Security Controls of the Criminal Investigation Management Information
System Have Not Been Implemented**

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Deputy Commissioner for Services and Enforcement SE
Chief, Mission Assurance OS:MA
Deputy Chief Financial Officer, Department of the Treasury

Key Security Controls of the Criminal Investigation Management Information System Have Not Been Implemented

Appendix IV

Management's Response to the Draft Report

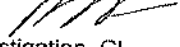


DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

March 18, 2004

RECEIVED
MAR 18 2004

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Nancy J. Jardini 
Chief, Criminal Investigation CI

SUBJECT: Response To Draft Audit Report—Key Security Controls of the Criminal Investigation Management Information System Have Not Been Implemented (Audit #200320012) ECMS IR No. 0402-5W4LMRBL

Criminal Investigation (CI) reviewed the Treasury Inspector General for Tax Administration (TIGTA) Draft Audit Report concerning the Criminal Investigation Management Information System (CIMIS). Your review of the CI CIMIS system and your recommendations will help guide CI toward improving our CIMIS system security. We have updated and replaced many of the network workstations that provide CIMIS access and are working to meet a March 2005 date to unveil a modern CIMIS system. Your recommendations will play a prominent part in the final security design for that new system.

Criminal Investigation takes seriously the security of our computer systems. As always, CI management will continue to enhance the security on the current CIMIS platform and will ensure that security concerns are addressed in the next generation of CIMIS. Additionally, CI management will reinforce to its field offices CI's existing policies and procedures related to CIMIS' security.

Our current CIMIS system, which is just one part of the entire CI network, falls into the "legacy system" category, which as noted by your auditors, is housed on older, out-dated equipment. Some of the security standards you noted may be difficult to meet in the manner you recommended. Implementing many of your recommendations on that equipment may not be feasible or cost-effective, given that the entire CIMIS system will be replaced in April 2005. During the interim, we will take all the steps necessary to ensure the security of the system and the data it contains. Those recommendations that we can implement will be done immediately. In other areas, we will do what can be done with the existing equipment to improve security and increase our monitoring of the system itself.

Key Security Controls of the Criminal Investigation Management Information System Have Not Been Implemented

2

Criminal Investigation personnel previously discussed many of your report's findings with your auditors and provided written responses to some of your conclusions and concerns. We have already taken corrective action on several findings you noted and will continue to work with Mission Assurance to address your other findings. For example, the auditors suggested that a more detailed inventory list be posted on the outside of the storage boxes. Criminal Investigation implemented the suggestion immediately. Additionally, CI has already implemented the recommendation to require the use of strong passwords throughout the CI network. Criminal Investigation also implemented the eight-character strong password as part of its standard sign-on procedures for all users on October 15, 2003.

Recommendation Comments

Recommendation one: In light of the auditors' findings, CI will review the current CIMIS Risk Assessment and Security Plan and make any updates and changes as required. Deficiencies discovered will be documented, corrected, and retained with the system documentation. CIMIS' security was recently recertified by Mission Assurance as part of the overall recertification of CI's electronic information network. Further, MITS did not have any issues or concerns when CIMIS was recertified through 2005. At that time, MITS was the certifying authority for IT systems, and remained such until Mission Assurance was formed in the late fall of 2003.

Finally, we note, both the CI network and CIMIS are being updated. System hardware and the CIMIS application are being replaced with a more modern and more secure environment that will meet or exceed the applicable risk and security standards. Reevaluating the certification of a legacy system that has a lifespan of a year or less should not be necessary, particularly given the review we are undertaking and the focus on the issues your audit report has provided.

Recommendation two: Criminal Investigation understands the importance of the Security Controls established in National Institute of Standards and Technology (NIST) Special Publication 800-18 and the requirements of Office of Management and Budget Circular A-130. Criminal Investigation will implement specific annual system security self-assessments outlined in Publication 800-26 and now required by Federal Information Security Act (FISMA) enacted in November 2002.

Criminal Investigation conducted a security assessment that applied the Publication 800-26 criteria. That assessment was done in a two-step process. The initial assessment used a form provided by the IRS Security Office that was based upon the NIST Publication 800-26 security self-assessment. The completed self-assessments were returned to the Security Office on August 14, 2003. On October 2, 2003, the Chief, CI, signed the FISMA Systems Security Assessment Validation Form provided by Security Policy Support and Oversight.

Recommendation three: Criminal Investigation has drafted and will soon be implementing new Form 5081 procedures and management will ensure that the new procedures will be followed with respect to all CIMIS user accounts.

Key Security Controls of the Criminal Investigation Management Information System Have Not Been Implemented

3

Recommendation four: Criminal Investigation will continue to emphasize that continuity of operations tests be performed annually. Full-scale annual testing will be instituted with the upgraded network and the new CIMIS system. The age and condition of the legacy CIMIS server made it difficult, if not impossible, to perform such testing without interrupting or irreparably damaging the existing system. We conducted those tests that would not have an adverse impact on operations, including purchasing a back-up server for testing, making periodic examination and documentation of the back-up tapes, and daily, off-site, mirrored back-up of the CIMIS data. Criminal Investigation has purchased a server that can emulate the current CIMIS server expressly to provide a reserve capacity for continuation of operations if the legacy server fails. We believe these steps are adequate to provide for the continuous operation of CIMIS under all conditions short of a full system failure.

Criminal Investigation is currently working with Mission Assurance on the Technical Contingency Planning Document (TCPD) for the CI network which includes CIMIS. The TCPD lists critical information about the CI network and systems such as CIMIS. The TCPD includes an Automated Data Processing Recovery Solution section that contains detailed information regarding recovery, such as critical application/system dependencies and back-up requirements, off-premise storage, recovery strategies and priorities, application/systems interim recovery strategy, as well as step-by-step recovery procedures and risk analysis. On January 13, 2004, we received approval on the TCPD document from the Acting Associate Director, Business Resilience Program Office of Mission Assurance.

Recommendation five: Criminal Investigation recognizes the importance of patch management and has a patch management process in place that distributes both operating system and security patches via the Systems Management Server (SMS) tool and CI's internal security program. Criminal Investigation's implementation of Windows XP on the workstations and the automated tool, which is available with Windows 2000/2003 server, enhances our ability to distribute and manage patches. The new CIMIS system will function within that same operating environment.

Criminal Investigation has been testing an automated tool for patch management. Information about the automated patch management tool was shared with your auditors. The automated tool for patch management, Microsoft (MS) Software Update Services (SUS), was successfully tested and is currently in the pilot phase. The MS SUS will allow CI to timely and automatically apply patches after testing.

Recommendation six: Criminal Investigation is working to strengthen its operating system controls for the CIMIS system. Although little can be done with the legacy CIMIS system, the rollout of the new system in 2005 will have adequate and robust controls. The deployment of Windows XP to all CI workstations (that has occurred since the audit was conducted) addresses many of the workstation security issues raised by the auditors. The specific recommendations made in the auditors' report have either been implemented or are under study. Criminal Investigation collaborates with MITS and attempts to follow the standard architecture as closely as possible. Criminal Investigation's workstations and servers are configured using the IRS' Law Enforcement Manual (LEM) requirements and LEM Checker scripts. When creating the CI Windows

Key Security Controls of the Criminal Investigation Management Information System Have Not Been Implemented

4

XP image, CI collaborated with the developers of the Common Operating Environment (COE) image and the CI image exceeds the security of the COE image. The XP rollout started in October 2003 and was completed in January 2004, as scheduled. Once Active Directory is implemented in 2004, CI will have the encrypted file system available for CI hardware.

Recommendation seven: Criminal Investigation has already taken steps to address this issue. The temporarily assigned CI Functional Security Officer has been analyzing the audit trail reports since November 2003. This analysis includes reviews for suspicious activity, such as unauthorized access and security violations. Further, he also downloads the audit trail reports to compact disks for permanent storage as suggested by your auditors. CI modified the existing direct root access procedures to provide for the "switch user" option and thus made provisions for sufficient user audit trails by system administrators. It should be noted that the announcement for the permanent CI Functional Security Officer closed on February 24, 2004, and it is expected that the position will be filled in the near future.

Other Comments

Criminal Investigation agrees with TIGTA that the draft audit report and CI's response should be classified as "Limited Official Use Information and Other Legends" and should be withheld from public disclosure.

Criminal Investigation's responses to the specific recommendations in the report are as follows:

Recommendation #1

The Chief, CI should take immediate steps to review and update the CIMIS risk assessment and security plan. Once these documents are amended to reflect the current security environment, they should be forwarded along with the results of our review to the Chief, Mission Assurance, to re-evaluate the current certification.

Corrective Action(s):

Criminal Investigation will review and update the CIMIS Risk Assessment and Security Plan, as required.

Implementation Date:

Completed _____ N/A _____ Proposed July 1, 2004 N/A _____

Responsible Official(s):

Director, Office of Strategy

Corrective Action(s) Monitoring Plan:

Upon review of the CIMIS Risk Assessment and Security Plan, an action plan will be formulated, if applicable.

Key Security Controls of the Criminal Investigation Management Information System Have Not Been Implemented

5

Recommendation #2

The Chief, CI should assess security controls annually by conducting tests in accordance with the NIST Special Publication 800-26, as required by the Office of Management and Budget and the Department of the Treasury.

Corrective Action(s):

Criminal Investigation will modify its security assessment procedures to specifically follow the NIST Special Publication 800-26 procedures and format.

Implementation Date:

Completed _____ N/A _____ Proposed July 1, 2004 N/A _____

Responsible Official(s):

Director, Office of Strategy

Corrective Action(s) Monitoring Plan:

The Director of Strategy will review changes to the security assessment procedures to ensure that this corrective action is met.

Recommendation #3

The Chief, CI should ensure a Form 5081 is used to create a user account and remind all CIMIS coordinators that all required information, including level of access, must be included on the Form 5081 before creating a CIMIS user account.

Corrective Action(s):

Criminal Investigation is already using the Form 5081, as well as the CIMIS/Criminal Investigation Equipment Inventory Control System (CIECS) User Request Form to create CIMIS user accounts. However, CI will develop procedures to use Form 5081 as the only vehicle for documenting approval of CIMIS user accounts. Because the current CIMIS/CIECS User Request Form encompasses more information than the Form 5081, CI will develop an internal process to ensure that additional information used by CI can be input in the "Special Instructions" section of Form 5081.

Implementation Date:

Completed _____ N/A _____ Proposed October 1, 2004 N/A _____

Responsible Official(s):

Director, Office of Strategy

Corrective Action(s) Monitoring Plan:

The CIMIS/CIECS User Request Form will be taken out of usage and the online Form 5081 process will become the only mechanism for requesting CIMIS user account actions.

Key Security Controls of the Criminal Investigation Management Information System Have Not Been Implemented

6

Recommendation #4

The Chief, CI should test the continuity of business operations on an annual basis.

Corrective Action(s):

Criminal Investigation will continue to emphasize that continuity of operations tests be performed annually and will develop formal testing procedure.

Implementation Date:

Completed _____ N/A _____ Proposed October 1, 2004 N/A _____

Responsible Official(s):

Director, Office of Strategy

Corrective Action(s) Monitoring Plan:

The Director, Office of Strategy will continue to ensure that continuity of operation tests are performed annually.

Recommendation #5

The Chief, CI should create a patch management process so that all applicable patches are identified, tested, and installed timely.

Corrective Action(s):

The implementation of MS Software Update Services tool will allow CI to put in place a more formal patch management process.

Implementation Date:

Completed _____ N/A _____ Proposed October 1, 2004 N/A _____

Responsible Official(s):

Director, Office of Strategy

Corrective Action(s) Monitoring Plan:

The Director, Office of Strategy will ensure that the implementation of the required software is completed within the prescribed timeframe.

Recommendation #6

The Chief, CI should strengthen the CI function's system administration responsibilities and take immediate action to ensure the operating system controls that support the CIMIS application conform to the rest of the IRS architecture.

Corrective Action(s):

The upgraded CIMIS System will include strengthened operating system control. Criminal Investigation will ensure that appropriate audit recommendations will be included in those controls.

Key Security Controls of the Criminal Investigation Management Information System Have Not Been Implemented

7

Implementation Date:

Completed _____ N/A _____ Proposed May 1, 2005 N/A _____

Responsible Official(s):

Director, Office of Strategy

Corrective Action(s) Monitoring Plan:

The Director, Office of Strategy will ensure that the upgraded CIMIS system includes strengthened operating controls.

Recommendation #7

The Chief, CI should ensure audit trail reports are run continuously and analyzed routinely by the Security Function Officer. Software used by other IRS functions can be used. Criminal Investigation operations staff, CI management, and the Security Function Officer should review the audit trail reports being implemented by the Chief, Mission Assurance, and implement them for audit trail analysis within the CI function. Close attention should be paid to high-risk activities such as employees signing on with root access.

Corrective Action(s):

Criminal Investigation is currently in the process of filling the permanent Security Officer position previously filled on a temporary basis. This should allow CI to assure that adequate audit trails are maintained and that logs are appropriately reviewed. The Security Officer will also have responsibility for ensuring that appropriate attention is given to high-risk activities.

Implementation Date:

Completed December 1, 2003 N/A _____ Proposed _____ N/A _____

Responsible Official(s):

Director, Office of Strategy

Corrective Action(s) Monitoring Plan:

The Director, Office of Strategy will continue to ensure that the temporarily and later the permanently assigned Security Officer maintain audit trails and logs.

If you have any questions, please call me at (202) 622-3200, or a member of your staff may contact Pota E. Coston, Director, Office of Strategy at (202) 622-5876.