The Internal Revenue Service Encrypts Data Transmitted Between Its Facilities, But Controls Over Cryptography Can Be Improved

October 2001

Report Number: 2002-20-007

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

INSPECTOR GENERAL
for TAX
ADMINISTRATION

October 11, 2001

MEMORANDUM FOR DEPUTY COMMISSIONER FOR MODERNIZATION &
CHIEF INFORMATION OFFICER

Pamela J Gardiner

FROM: Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Final Audit Report - The Internal Revenue Service Encrypts Data Transmitted Between Its Facilities, But Controls Over Cryptography Can Be Improved (Audit # 200120004)

This report represents the results of our review of the Internal Revenue Service's (IRS) controls over its implementation of encryption. In summary, we found that the circuits over which the most significant volume of IRS data passes *between* facilities are encrypted. However, we identified risk areas that require the attention of IRS management. The IRS has not developed or implemented policies and procedures regarding encryption and its application within the agency. In addition, the IRS should assess the risks of transmitting unencrypted data *within* its facilities. Lastly, although the IRS has made progress in replacing outdated encryption devices, a significant number of circuits are encrypted with aging equipment that no longer meet government standards.

We recommended that the Deputy Commissioner for Modernization & Chief Information Officer (CIO) should ensure that an overall encryption strategy for the IRS, including an encryption plan, is developed and specific encryption policies and procedures are defined and enforced. In addition, the Deputy Commissioner for Modernization & CIO should conduct a risk analysis of information transmitted unencrypted within IRS facilities and establish plans to remove outdated encryption equipment from service. Management agreed with our recommendations and developed appropriate corrective actions. Management's comments have been incorporated into the report where appropriate, and the full text of their comments is included as Appendix V.

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 Unit 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 Scott E. Wilson, Assistant Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

Table of Contents

Executive Summary

Risks to the security of our government's computer systems are significant and they are growing. One area of risk is the protection of electronic data transmissions. With the advent of new and inexpensive technology, it is becoming easier for individuals or groups to obtain information for which they are not the intended recipients. An important part of the solution to this security concern is cryptography[1] or encryption. Encryption is the encoding of information so that only an intended recipient can read it. Information that has been properly encrypted cannot be understood or interpreted by those lacking the appropriate cryptographic key. While information vulnerabilities cannot be eliminated through the use of any single tool, cryptography can help ensure the confidentiality and integrity of information in transit.

This report presents the results of our review of the Internal Revenue Service's (IRS) encryption policies and procedures and their effectiveness in protecting data transmitted over its various networks. We conducted this review on various segments of the IRS' network. The objective of this review was to evaluate the IRS' encryption policies and procedures and verify that they are properly implemented to ensure that sensitive internal and taxpayer data are adequately protected.

Results

The circuits over which the most significant volume of IRS data pass are encrypted because the IRS has the structure in place to encrypt data transmissions between its computing centers, service centers, and large posts-of-duty. We did not identify any instances where encryption was turned off. However, we identified risk areas that require the attention of IRS management.

The Internal Revenue Service Should Establish Detailed Policies and Procedures Regarding Encryption and Its Application Within the Agency

The IRS has extensively implemented encryption to protect the transmission of taxpayer data, but has not taken steps to assure encryption is operating as intended. For encryption to work properly, an organization must take steps to assure that unauthorized individuals do not have access to encryption equipment or information, such as

[1] Cryptography is the enciphering and deciphering of messages in secret code or cipher.

cryptographic keys or hardware manuals, that could be used to decrypt data. The IRS has not established detailed policies and procedures for the management of encryption and all communications security material.[2] Policies and procedures are necessary for both encryption services obtained through the Treasury Communications System[3] and locally controlled encryption services to assure the continued secure transmission of data between IRS sites.

The Internal Revenue Service Should Conduct a Risk Analysis To Identify Data Transmissions Requiring Special Protection

Although the IRS has established a policy that all data transmitted from its facilities must be encrypted, the IRS has not assessed the risk that sensitive data transmitted over all its internal networks may be compromised. The unencrypted internal transmission of data can result in unauthorized disclosure of personnel information or other more critical system data of use to a malicious insider. Modern technology has made it relatively easy for a knowledgeable insider to eavesdrop on internal data transmissions and messages. In order to avoid unwanted internal disclosures of sensitive data, the IRS must identify the varying degrees of data sensitivity and implement the required protection for the data that is transmitted inside IRS facilities.

Outdated Encryption Equipment Continues To Be Employed Throughout the Internal Revenue Service

The IRS has had to replace a great deal of its outdated encryption equipment, but it continues to have significant numbers of obsolete equipment and has not established specific plans to retire them. In addition, a crucial step in the regular maintenance of these obsolete machines, manually changing the cryptographic key, has been suspended. The periodic changing of the key is needed because, with technological advances, it has become increasingly possible that Data Encryption Standard (DES)[4] encrypted text can

[2] Communications Security, or COMSEC, consists of measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications. With regard to encryption, COMSEC material includes encryption keys, equipment, manuals, and devices that must be kept under strict control and be tracked.

[3] The Treasury Communications System program was established to provide Treasury's bureaus and its departmental offices with a variety of data communications services through a single contract vehicle. Its purpose is to provide a centralized network and management system to support its customers' missions by providing a wide range of data communications services.

[4] DES is an encryption algorithm that the government previously endorsed but has recommended be replaced with a new standard, Triple DES.

be broken and, thus, compromised or disclosed. Although the IRS recognizes that the outdated equipment needs to be replaced, it needs to develop and monitor plans for its retirement

Summary of Recommendations

The Deputy Commissioner for Modernization & Chief Information Officer (CIO) should ensure that an encryption plan is developed and specific encryption policies and procedures are defined and enforced. In addition, the Deputy Commissioner for Modernization & CIO should conduct a risk analysis of information transmitted unencrypted within IRS facilities and establish plans to remove outdated encryption equipment from service.

Management's Response: IRS management will develop policies for managing and controlling encryption and communicating security material. In addition, IRS management has conducted vulnerability assessments showing a need for additional controls to manage network diagnostic tools and is developing operations security guidelines, standards, and procedures governing the use of such tools.

IRS management is also establishing commitments with the Department of the Treasury and other bureaus to phase out current DES technology and is migrating from current dedicated circuits that employ DES encryption to a Triple DES solution.

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

Objective and Scope

The objective of this review was to evaluate the IRS' encryption policies and procedures and verify that they are properly implemented to ensure that sensitive internal and taxpayer data are adequately protected.

This report presents the results of our review of the Internal Revenue Service's (IRS) encryption policies and procedures and their effectiveness in protecting data transmitted over its various networks. We conducted this review on various segments of the IRS' network. The objective of this review was to evaluate the IRS' encryption policies and procedures and verify that they are properly implemented to ensure that sensitive internal and taxpayer data are adequately protected.

We conducted this review within the Office of the Deputy Commissioner for Modernization & Chief Information Officer (CIO) and within the Department of the Treasury's Treasury Communications System (TCS).[1] We performed interviews in the National Headquarters, and audit tests were completed on the IRS networks at the Martinsburg Computing Center (MCC) in Kearneysville, West Virginia, at IRS sites in the Atlanta, Georgia metropolitan area, at IRS sites in the Cincinnati, Ohio/Covington, Kentucky metropolitan area, and at the TCS facility in McLean, Virginia. Specific sites are included in Appendix IV. Fieldwork was conducted from January to June 2001. This audit was performed in accordance with *Government Auditing Standards.*

Details of our objective, scope, and methodology are presented in Appendix I. Major contributors to this report are listed in Appendix II.

[1] The Treasury Communications System program was established to provide Treasury's bureaus and its departmental offices with a variety of data communications services through a single contract vehicle. Its purpose is to provide a centralized network and management system to support its customers' missions by providing a wide range of data communications services.

Background

According to Congressional testimony from the General Accounting Office in September 1999,[2] risks to the security of our government's computer systems are significant and they are growing. The dramatic increase of computer interconnectivity and the popularity of the Internet, while facilitating access to information, are factors that also make controls over access to information more important. One risk is the protection of electronic data transmissions. The advent of network sniffer, or eavesdropping, technology has made it easier for individuals and groups with malicious intentions to obtain information allowing them to intrude into inadequately protected systems.

System break-ins at the Department of the Treasury could place billions of dollars of annual federal receipts and payments at risk of fraud and large amounts of sensitive taxpayer data at risk of inappropriate disclosure.

Attacks on and misuse of federal computer and telecommunications resources are of increasing concern because these resources are virtually indispensable for carrying out critical operations and protecting sensitive data and assets. For example, system break-ins at the Department of the Treasury could place billions of dollars of annual federal receipts and payments at risk of fraud and large amounts of sensitive taxpayer data at risk of inappropriate disclosure. In Fiscal Year 2000, the IRS collected over $2 trillion in taxes, processed over 210 million tax returns, and paid about $194 billion in refunds to taxpayers.[3]

The need to protect sensitive data and systems must be weighed not only against cost and feasibility concerns, but also the privacy and security interests of individual

[2] United States General Accounting Office Testimony Before the Subcommittee on Technology, Committee on Science, House of Representatives, September 30, 1999 (GAO/T-AIMD-99-302).

[3] United States General Accounting Office Report to the Secretary of the Treasury, FINANCIAL AUDIT, IRS' Fiscal Year 2000 Financial Statements (GAO-01-394, dated March 2001).

citizens and private businesses, as well as national security and law enforcement agencies. An important part of the solution to these security concerns is cryptography[4] or encryption. Encryption is the encoding of information so that only an intended recipient can read it. Information that has been properly authenticated and encrypted cannot be understood or interpreted by those lacking the appropriate cryptographic key. While information vulnerabilities cannot be eliminated through the use of any single tool, cryptography can help ensure the confidentiality and integrity of information in transit.

Information that has been properly authenticated and encrypted cannot be understood or interpreted by those lacking the appropriate cryptographic key.

Large portions of the IRS' encryption needs are met through the TCS. The TCS was established to provide Treasury's bureaus and its departmental offices with a variety of data communications services through a single contract vehicle. The contract, awarded in September 1995 to TRW Inc., is intended for the design, implementation, management, operation, maintenance, and enhancement of a data communications network for the Department of the Treasury and its bureaus.

Results

The circuits over which the most significant volume of IRS data pass are encrypted because the IRS has the structure in place to encrypt data transmissions between its computing centers, service centers, and large posts-of-duty. We did not identify any instances where encryption was turned off. We also determined that, for circuits where encryption services are provided through the TCS, a system is in place that detects and assists in the resolution of encryption problems. We did identify one circuit without encryption for which the IRS ordered

[4] Cryptography is the enciphering and deciphering of messages in secret code or cipher.

encryption after we identified the situation. We also identified other risk areas that require the attention of IRS management.

The IRS is responsible for developing an overall encryption strategy, and completing policies and specific procedures for the control of communication security materials.

Although the IRS relies heavily on the TCS for encryption services, the IRS is responsible for developing an overall encryption strategy and completing policies and specific procedures for the control of communication security materials. However, the IRS has not prepared an overall encryption strategy and adequately communicated policies and procedures to its telecommunications technicians in its operations sites. Specifically:

- For circuits where the TCS provides encryption services, the IRS still must define the internal responsibilities for the day-to-day handling of communications security materials and the interaction with TCS personnel and contractors.
- For circuits not acquired through the TCS, guidance for all aspects of encryption management and communications security is necessary.

In addition, we determined that the IRS has not analyzed its data transmissions and assessed the risks of disclosure to unauthorized personnel within its facilities. Data within IRS facilities are generally not encrypted, even though some of that data should only be known to individuals exchanging that data. A risk assessment of these data transmissions within an IRS facility has not been conducted. This risk assessment is needed to identify internally transmitted information that requires the same encryption protection as is used for transmission of data between IRS sites.

Lastly, although the IRS has made progress in replacing outdated encryption devices, a significant number of circuits are encrypted with aging equipment that no longer meet government standards.

The Internal Revenue Service Should Establish Detailed Policies and Procedures Regarding Encryption and Its Application Within the Agency

Although the IRS has extensively implemented encryption to protect the transmission of taxpayer data, it has not taken steps to assure encryption is operating as intended. For encryption to work properly, an organization must take steps to assure that unauthorized individuals do not have access to encryption equipment or information, such as cryptographic keys or hardware manuals, that could be used to decrypt data. The IRS has not established detailed policies and procedures for the management of encryption and all communications security material.[5] We determined through our field visits that policies and procedures have not been written and distributed to IRS personnel charged with the everyday observation and handling of encryption devices and associated communications security material.

Policies and procedures are necessary for both encryption services obtained through the TCS and locally controlled encryption services.

We identified two different conditions for which the IRS needs to develop policies and procedures. These policies and procedures are necessary for both encryption services obtained through the TCS and locally controlled encryption services to assure the continued secure transmission of data between IRS sites.

[5] Communications Security, or COMSEC, consists of measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications. With regard to encryption, COMSEC material includes encryption keys, equipment, manuals, and devices that must be kept under strict control and be tracked.

Procedures are necessary for encryption services procured through the TCS

These procedures are needed to assist local IRS telecommunications technicians in the day-to-day handling of the communications security equipment and interaction with the TCS contractor and subcontractor personnel to assure proper monitoring and maintenance of encryption equipment. Such detailed procedures should include escalation procedures for troubleshooting encryption units, procedures to authenticate and monitor technicians working in IRS facilities, and notification and recordation requirements for encryption-related problems. Without such procedures, the IRS abdicates control of all communication security, an inherently governmental responsibility, to contractor personnel.

The lack of adequate direction for telecommunications technicians has resulted in practices that can compromise encryption.

The lack of adequate direction for telecommunications technicians has resulted in practices that can compromise encryption. Specifically:

- Access to areas housing encryption equipment is not always properly controlled. For example, at one site, we found that contractors could enter these areas without IRS supervision.
- Encryption devices when housed in large computer rooms were not locked or segregated from the rest of the room. In addition, at one site we found unsecured encryption devices located outside of a computer room or telecommunications closet.
- Telecommunications technicians in the field did not always properly clear encryption equipment of encryption keys (zeroized) prior to removing them from IRS sites.

Except for one site, MCC, we did not identify adequate escalation procedures for the handling of encryption problems. At times in the course of troubleshooting an encryption-related problem, the encryption unit will be placed in bypass mode or, in other words, taken off-line. In extreme cases, unencrypted data may need to be passed over a circuit. There should be procedures to define the steps necessary to place encryptors in bypass mode and the approvals necessary to run data unencrypted over a circuit.

The procedures developed at the MCC serve as an example of what procedures should contain. They specified that a trouble ticket should be initiated to track the problem, defined information that should be included in the ticket, required entries in a separate log, and named specific individuals to notify and request approval for transmission of data over an unencrypted circuit. This type of detailed procedure was not found in the other sites we visited.

Policy must also be provided for situations where circuits and encryption services are not procured through the TCS

In Atlanta, we identified eight local circuits where encryption was handled entirely by local technicians. No procedures were available to these employees for handling, initializing, monitoring, or maintaining these devices. As a result, the machines employed only DES encryption;[6] were not regularly re-keyed; and spare communications security equipment, including encryptors with their keys and manuals, were stored on the computer room floor. Such exposures could facilitate data decryption efforts by an unauthorized individual.

The need for encryption policies is established in federal and departmental guidance. The Federal Information Processing Standards Publication (FIPS PUB) 140-2, Security Requirements for Cryptographic Modules Section 4.10.4, establishes the need for guidance documents. It states that user guidance should describe

[6] DES is an encryption algorithm that the government previously endorsed but has recommended be replaced with a new standard, Triple DES.

The user guidance documentation should describe all user responsibilities necessary for the secure operation of the cryptographic module.

the security functions of the cryptographic module along with instructions, guidelines, and warnings for its secure use. The user guidance documentation should describe all user responsibilities necessary for the secure operation of the cryptographic module and, if applicable, a description of all security requirements for the information technology environment that are relevant to the user. Treasury Directive 71-10 extends these requirements stating that all bureaus and offices with sensitive but unclassified (SBU) applications should develop an encryption plan for all telecommunications. An encryption plan is used to articulate a strategy for secure data transmission. Specific requirements for the plan are detailed in the directive.

The IRS has broadly addressed encryption in its Internal Revenue Manual (IRM). The IRM states that IRS data is SBU and all transmissions of SBU data must be encrypted. Generally, the IRM establishes the need for encryption but provides few details for encryption-related responsibilities and tasks. We found additional fragmented, locally-developed procedures in some of the sites where we conducted fieldwork. However, none of the locally-developed procedures provided the detail needed to assure encryption services are not compromised.

There are several reasons why encryption policies and procedures have not been established.

There are several reasons why these policies and procedures have not been established:

- Responsibility for encryption policies and procedures within the IRS has not been defined. Discussions with various IRS organizations did not identify any additional policies or procedures beyond those included in the IRM.
- The IRS has not developed an encryption plan in accordance with Treasury Directive 71-10. Such a plan includes defining a strategy for controlling data encryption.

- IRS organizations believe that encryption services are provided through the TCS, and policies and procedures for such should be produced by the contractor.
- Treasury assigns responsibility to each of the individual Treasury bureaus to develop and distribute their own policies and procedures regarding encryption. Treasury personnel indicated that they have no authority to enforce policies within the bureaus, and to date, have not written policies and procedures for the bureaus.

Recommendations

1. The Deputy Commissioner for Modernization & Chief Information Officer (CIO) should identify the organization with responsibility for developing policies and procedures governing the management and control of encryption and communications security material.

Management's Response: IRS management stated that the Office of Security Evaluation and Oversight (SEO) is responsible for developing policies for managing and controlling encryption and communicating security material.

2. The Deputy Commissioner for Modernization & CIO should identify the organization responsible for implementing and enforcing the policies and procedures for the management and control of communications security material.

Management's Response: IRS management stated that the Office of Telecommunications is responsible for implementing policies and procedures for managing and controlling communications security material. The Office of SEO is responsible for implementing these policies. The SEO will continue to evaluate the management controls over encryption and communications security material during its security reviews.

3. The Deputy Commissioner for Modernization & CIO should ensure that encryption policies and procedures are enforced.

Management's Response: IRS management stated that the Office of SEO will continue to evaluate the management controls over encryption and communications security material during its security reviews. IRS management documented, controlled, and coordinated vulnerabilities the Office of SEO identified with the Office of Telecommunications and local sites until the responsible organization completes the corrective action(s).

4. The Deputy Commissioner for Modernization & CIO should ensure that an encryption plan is developed for the IRS.

Management's Response: IRS management stated that the Office of SEO and the Office of Telecommunications are jointly developing operations security guidelines, standards, and procedures (GSP) not included in other documents. This GSP will include the IRS encryption plan and other related documents. The Office of Telecommunications will implement the guidelines through IRS field offices responsible for telecommunication support.

The Internal Revenue Service Should Conduct a Risk Analysis To Identify Data Transmissions Requiring Special Protection

Modern technology has made it relatively easy for a knowledgeable insider to eavesdrop on internal data transmissions and messages.

Although the IRS has established a policy that all data transmitted from its facilities must be encrypted, the IRS has not assessed the risk that sensitive data transmitted over its internal networks may be compromised. Modern technology has made it relatively easy for a knowledgeable insider to eavesdrop on internal data transmissions and messages. In order to avoid unwanted internal disclosures of sensitive data, the IRS should identify the varying degrees of data sensitivity and implement the required protection for the data that is transmitted inside IRS facilities

Treasury Directive 71-10 states that all bureaus and offices shall implement encryption on those telecommunications and information systems transmitting classified national security information and identify those systems transmitting SBU information that may require protection. This determination should be based on a risk analysis to identify threats to and vulnerabilities of the system. These systems should incorporate approved protection techniques consistent with applicable departmental Office of Security policies in the most cost-effective manner. The IRM requires that encryption be used for transmitting SBU information between IRS facilities when not using the Treasury network, which is encrypted.

Data is not encrypted when it is transmitted inside IRS facilities.

While data is encrypted just prior to exiting one IRS site and is decrypted immediately upon entering another IRS site, data is not encrypted when it is transmitted inside IRS facilities. The encryption of data between sites is referred to as link encryption. Although an adequate protection for a large portion of the IRS' data, link encryption may not be sufficient because it provides no encryption for some types of information transmitted internally such as personnel information or sensitive system information that may need to be encrypted. The internal communications include unencrypted email messages that may be used to transmit sensitive information. The IRS has undertaken an initiative that will address unencrypted email, but this project is currently in the pilot phase.

The IRS has not conducted a risk analysis of data transmitted over its internal networks to determine whether any data transmitted within a facility needs to be encrypted. In some cases, such IRS facilities may have several thousand employees who are exchanging information on unencrypted internal networks. Although the IRS assesses data protection requirements on a project-by-project basis for certification, it has not performed an assessment that considers the security requirements for all the types of data found in its system. In our view, link encryption is adequate for the transmitting of taxpayer data. However, other data needs to be assessed to determine if it should be encrypted when transmitted within IRS facilities.

Network "sniffers" can be implemented on an internal local area network and used to identify specific traffic that can be intercepted by individuals seeking to obtain information they would normally not be able to access.

The unencrypted internal transmission of these types of data can result in unauthorized disclosure of personnel information or other more critical system data of use to a malicious insider. Current network "sniffer" technology is relatively inexpensive. Sniffers can be implemented on an internal local area network and used to identify specific traffic that can be intercepted by individuals seeking to obtain information they would normally not be able to access. If these data files are not encrypted, the interceptor can read the clear text files the same as the intended recipient.

Recommendation

5. The Deputy Commissioner for Modernization & CIO should conduct a risk analysis to identify any information transmitted over the IRS network that may require protection beyond what is currently

provided through its link encryption. Results of this risk analysis should clearly identify specific data transmissions that require additional protection within IRS facilities beyond those that will be handled through the current email initiative.

Management's Response: IRS management stated that owners of all applications and systems that process, transmit, or store sensitive but unclassified data must have a risk assessment and security plan in place (and updated at least every 3 years) before they receive a security certification. In these documents, a data sensitivity analysis and requisite risk mitigation requirements were identified as well as any point-to-point encryption requirement.

The Office of SEO conducted vulnerability assessments showing that the IRS needs additional controls to manage network diagnostic tools. The Office of SEO is developing operations security guidelines, standards, and procedures governing the use of data scopes (sniffers/analyzers) and network scanning tools.

The Office of Telecommunications will implement and enforce the guidelines.

Outdated Encryption Equipment Continues To Be Employed Throughout the Internal Revenue Service

Although the IRS recognizes that the outdated equipment needs to be replaced, it needs to develop and monitor plans for its retirement.

The IRS has had to replace a great deal of its outdated encryption equipment, but it continues to have significant numbers of obsolete equipment and has not established specific plans to retire them. In addition, a crucial step in the regular maintenance of these obsolete machines, manually changing the cryptographic key, has been suspended. The periodic changing of the key is needed because, with technological advances, it has become increasingly possible that DES-encrypted text can be "broken" and, thus, compromised or disclosed. Although the IRS recognizes that the outdated equipment needs to be replaced, it needs to develop and monitor plans for its retirement.

Treasury bureaus were informed in July 1998 that encryption equipment employing a DES algorithm was no longer safe. Since that time, the IRS has made changes that decreased the number of obsolete encryption devices in use, but significant numbers of the outdated devices remain in use. Although the IRS' inventory of encryption devices is in flux due to the implementation of new telecommunications technology, an inventory obtained from the TCS showed 604 encryptors of one specific non-compliant model in use at the IRS on April 27, 2001. Our review of encryption equipment at various sites showed that it is likely that the IRS is using other non-compliant devices. Since these models can be configured using different encryption algorithms, we did not perform an extensive device-by-device analysis to identify all the non-compliant encryption equipment.

Currently, the IRS uses DES encryptors for its mainframe data transmissions between its computing centers and service centers.

Currently, the IRS uses DES encryptors for one of the major segments of its mainframe data transmissions between computing centers and service centers. The IRS continues to work on a plan to migrate data traffic off of this equipment onto equipment that meets standards, but specific time frames for this replacement have not been established.

In the three cities where we conducted fieldwork, we found circuits that connect two IRS sites encrypted with DES devices. Specifically, we identified:

- 56 circuits at the MCC.
- 36 circuits in the Atlanta metropolitan area sites.
- 23 circuits in the Cincinnati/Covington metropolitan area sites.

In addition, we found DES units on 22 other circuits in Atlanta and 44 other circuits in Cincinnati awaiting deinstallation. These circuits are part of an earlier version of a shared Treasury network, but are still housed in IRS facilities.

When encryption is operating as intended, readable data can be recovered from the encrypted data only by using exactly the same key used to encrypt it. Unauthorized recipients of the encrypted data who know the algorithm but do not have the correct key cannot derive the original data algorithmically. However, it may be feasible to determine the key through a brute force "exhaustion attack," i.e., breaking a DES-encrypted message by trying all possible keys. By determining the correct key and having the DES algorithm, the encrypted data can be de-encrypted and the original data obtained.

A successful brute force attack occurred in 1998. The DES Cracker Project[7] broke a DES-encrypted message using a system requiring a relatively small investment for a determined organization planning the destruction or misuse of a given system. Thus, the IRS and the data it transmits using DES encryption is increasingly at risk of compromise and disclosure.

The NIST advises agencies that the government can no longer support the use of DES for many applications because of the success of the DES key attack.

The National Institute of Standards and Technology (NIST) advises agencies that the government can no longer support the use of DES for many applications because of the success of the DES key attack. The NIST FIPS-PUB 46-3 encourages government agencies still employing DES systems to transition to Triple DES encryption devices and directs them to implement Triple DES devices for new development. Although the NIST did not establish a date by which DES systems must be replaced, the advances in technology since 1998 and the rapidly decreasing costs for information technology

[7] The DES Cracker Project was a joint effort by the Electronic Freedom Foundation, Advanced Technologies Inc., and Cryptography Research Inc. conducted in 1998.

warrant a plan that specifies when replacement can be expected.

The Department of the Treasury made its bureaus aware of the problem with DES equipment in a memo issued in July 1998. Treasury's Office of Systems Security issued the memo stating the results of the DES Cracker Project and provided recommendations to bureaus. The recommendations included the implementation of shorter periods between manual re-keying of DES-based encryption, ending procurement of additional DES equipment, and phasing out DES products at the end of their useful life.

Although this directive has been in place for 3 years, the Treasury and the IRS do not have agreed upon plans for the replacement of the obsolete encryption equipment. Although the IRS has migrated applications off of the earlier version of the shared Treasury network, other Treasury bureaus still employ the network and are dependent on the equipment that exists in IRS facilities. IRS management indicated that budget constraints and Treasury priorities have contributed to the continued use of this equipment.

Recommendation

6. The Deputy Commissioner for Modernization & CIO should establish realistic commitments to phase out current DES technology. This phase out should include:

   a. The final dissolution of the first shared Treasury network circuitry and destruction of the associated DES encryption equipment.

   b. The migration of the major segment of mainframe communications between computing centers and service centers from the current dedicated circuits that employ DES encryption to a Triple DES solution.

Management's Response: IRS management stated that the Office of Telecommunications is establishing commitments with the Department of the Treasury and other bureaus to phase out current DES technology. This will include the final dissolution of the first shared Treasury network circuitry and the destruction of the associated DES encryption equipment. It will also include migrating the major segment of mainframe communications between computing centers and service centers from the current dedicated circuits that employ DES encryption to a Triple DES solution.

Conclusion

With the increasing threats to computer systems and specifically data transmissions, government organizations must implement controls that mitigate risks and assure that data are only available to intended recipients. The IRS has implemented a structure to encrypt data transmissions between its facilities. However, the IRS should institute policies and procedures that assure its contractors and government personnel properly administer encryption. In addition, further considerations of internal data transmissions and the retirement of obsolete equipment are necessary for the strengthening of the IRS' encryption controls.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to evaluate the Internal Revenue Service's (IRS) encryption policies and procedures and verify that they are properly implemented to ensure that sensitive internal and taxpayer data are adequately protected. Specifically, we:

I. Determined whether the IRS' encryption policies and procedures were adequate to ensure protection of its electronic data interchanges.

   A. Identified industry best practices for managing cryptography[1] in a large enterprise.

   B. Identified the policies and procedures that govern electronic data interchange for the IRS.

   C. Determined whether the IRS' existing policies and procedures were current with regard to policies developed by the Department of the Treasury and other standards making organizations [for example, the National Security Agency and the National Institute of Standards and Technology (NIST)].

   D. Determined whether the roles and responsibilities of the various IRS organizations adequately addressed encryption for all areas where sensitive data is electronically transmitted.

   E. Determined whether policies existed for specific electronic data interchanges in the IRS.

II. Determined whether the circuits over which the most significant amounts of IRS data pass (circuits between the computing centers and service centers) were properly encrypted.

   A. Determined whether these circuits were acquired through the Treasury Communications System (TCS).

   B. Determined whether encryption was adequately managed on the circuits acquired through the TCS.

[1] Cryptography is the enciphering and deciphering of messages in secret code or cipher.

C. Determined whether the Department of the Treasury tests or monitors encryption on the TCS.

III. Determined how the IRS managed encryption on circuits not purchased through the TCS.

A. Determined to what extent these circuits were encrypted.

B. Determined whether key management practices were adequate to ensure encryption devices cannot be easily comprised.

C. Determined whether procedures were adequate to ensure instances of encryption bypass were minimized and timely rectified.

IV. Determined whether the NIST-approved encryption devices were used by the IRS.

A. For the sites we visited, we determined whether the devices used met current NIST guidelines.

B. Determined whether current upgrade or modernization plans addressed any deficiencies noted in IV.A.

C. Where plans were identified in IV.B, we determined the status and time frame for completion of the efforts to rectify any deficiencies.

Appendix II

Major Contributors to This Report

Scott E. Wilson, Assistant Inspector General for Audit (Information Systems Programs)
Gary Hinkle, Director
Vincent Dell'Orto, Audit Manager
Anthony Knox, Senior Auditor
Tina Wong, Auditor

Appendix III

Report Distribution List

Commissioner N:C
Deputy Assistant Secretary (Information Systems) and Chief Information Officer,
Department of the Treasury MI
Deputy Chief Financial Officer, Department of the Treasury
Chief, Information Technology Services M:I
Director, Corporate Computing M:I:E
Director, Martinsburg Computing Center M:I:E:MC
Director, Telecommunications M:I:T
Director, Desktop Management M:I:F
Director, Office of Security M:S
Director, Office of Security Evaluation and Oversight M:S:S
Director, Strategic Planning and Client Services M:SP

Appendix IV

Fieldwork Site List

Atlanta Campus
Doraville, Georgia

Cincinnati Campus
Covington, Kentucky

Martinsburg Computing Center
Kearneysville, West Virginia

Treasury Communications System
McLean, Virginia

Internal Revenue Service Field Sites:
401 West Peachtree Street NW, Atlanta, Georgia

550 Main Street, Cincinnati, Ohio

2888 Woodcock Boulevard, Atlanta, Georgia

Appendix V

Management's Response to the Draft Report

LIMITED OFFICIAL USE

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

DEPUTY COMMISSIONER

SEP 27 2001

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

John C. Reece

FROM: John C. Reece
Deputy Commissioner of Modernization &
Chief Information Officer

SUBJECT: Response to Draft Report – The IRS Encrypts Data Transmitted Between Its Facilities, But Controls Over Cryptography Can Be Improved (Audit No. 200120004)

Thank you for the opportunity to review and comment on your draft report and recommendations about our encryption of electronic data transmissions.

In your report, you stated that although circuits over which the most significant volume of IRS data passes are encrypted, you identified risks. Our security program is focused on effectively managing risks. Therefore, we now have managers and processes in place and corrective actions underway, to implement your recommendations. I have attached a detailed response to each of your recommendations.

I appreciate your comments. They will help us strengthen our encryption security controls. If you have any questions or concerns, please contact me at (202) 622-6800 or Mr. Len Baptiste, Director, Office of IRS-Wide Security at (202) 622-8910.

Attachment

LIMITED OFFICIAL USE

LIMITED OFFICIAL USE

Attachment

Management response to Draft Audit Report – The Internal Revenue Service Encrypts Data Transmitted Between Its Facilities, But Controls Over Cryptography Can Be Improved (#200120004)

RECOMMENDATION #1:

The Deputy Commissioner for Modernization & Chief Information Officer (CIO) should identify the organization with responsibility for developing policies and procedures governing the management and control of encryption and communications security material.

ASSESSMENT OF CAUSE:

We had not adequately defined the responsibility for encryption policies within the IRS.

CORRECTIVE ACTION TO RECOMMENDATION #1:

We have identified the responsible organizations. The Office of Security Evaluation and Oversight (SEO) is responsible for developing policies for managing and controlling encryption and communicating security material. The Office of Security Evaluation and Oversight and the Office of Telecommunications are jointly developing operations security guidelines, standards, and procedures (GSP) not included in other documents. The GSP will also help implement procedures to manage and control encryption and communicate security material. We will track this part of the corrective action under recommendation #4 of this report.

IMPLEMENTATION DATE: Completed

RESPONSIBLE OFFICIAL:

Director, Office of Security Evaluation and Oversight, M:S:S
Director, Office of Telecommunications, M:I:T

LIMITED OFFICIAL USE

RECOMMENDATION #2:

The Deputy Commissioner for Modernization & CIO should identify the organization responsible for implementing and enforcing the policies and procedures for the management and control of communications security material.

ASSESSMENT OF CAUSE:

We had not adequately defined the responsibility for implementing procedures in support of the IRS encryption policy.

CORRECTIVE ACTION TO RECOMMENDATION #2:

We have identified the responsible organizations. The Office of Telecommunications is responsible for implementing policies and procedures for managing and controlling communications security material. The Office of Security Evaluation and Oversight is responsible for implementing these policies. The Office of Security Evaluation and Oversight will continue to evaluate the management controls over encryption and communications security materials during its security reviews.

IMPLEMENTATION DATE: Completed

RESPONSIBLE OFFICIAL:

Director, Office of Telecommunications, M:I:T
Director, Office of Security Evaluation and Oversight, M:S:S

RECOMMENDATION #3:

The Deputy Commissioner for Modernization & CIO should ensure that encryption policies and procedures are enforced.

ASSESSMENT OF CAUSE:

- Sites with existing IRS policies and procedures did not comply with IS encryption policies and procedures.
- IRS field locations did not have sufficient Internal Revenue Manual or operational procedures to establish clear expectations in all of the areas that support the operational use of encryption to protect taxpayer data.

CORRECTIVE ACTION TO RECOMMENDATION #3:

During its security reviews, the Office of Security Evaluation and Oversight will continue to evaluate the management controls over encryption and communications security material. We documented, controlled, and coordinate vulnerabilities the SEO identified with the Office of Telecommunications and local sites until the responsible organization has completed the corrective action(s).

We are developing the additional documentation needed by local site management to enhance compliance and have addressed it in our corrective action to recommendation #4 of this report.

IMPLEMENTATION DATE: Completed

RESPONSIBLE OFFICIAL:

Director, Office of Security Evaluation and Oversight, M:S:S

RECOMMENDATION #4:

The Deputy Commissioner for Modernization & CIO should ensure that an encryption plan is developed for the IRS.

ASSESSMENT OF CAUSE:

While IRS has identified much of its encryption requirements in the Internal Revenue Manual, the IRS has not developed an encryption plan in accordance with Treasury Directive 71-10. Such a plan includes detailed policies and procedures regarding encryption and includes defining a strategy for controlling data encryption.

CORRECTIVE ACTION TO RECOMMENDATION #4:

We are working to correct this weakness. The Office of Security Evaluation and Oversight and the Office of Telecommunications are jointly developing operations security guidelines, standards and procedures (GSP) not included in other documents. This GSP will include the IRS encryption plan and other related documents. The Office of Telecommunications will implement the guidelines through IRS field offices responsible for telecommunication support.

IMPLEMENTATION DATE:

Develop guidelines: December 2001

Implement guidelines Service-wide: July 2002

RESPONSIBLE OFFICIAL:

Develop guidelines: Director, Office of Security Evaluation and Oversight, M:S:S

Implement guidelines: Director, Office of Telecommunications, M:I:T

LIMITED OFFICIAL USE

RECOMMENDATION #5:

The Deputy Commissioner for Modernization & CIO should conduct a risk analysis to identify any information transmitted over the IRS network that may require protection beyond what is currently provided through its link encryption. Results of this risk analysis should clearly identify specific data transmissions that require additional protection within IRS facilities beyond those that will be handled through the current email initiative.

ASSESSMENT OF CAUSE:

IRS has established a policy that we will encrypt all data transmitted from our facilities and perform vulnerability assessments, but we have not fully addressed the risk that sensitive data transmitted over our internal networks could be compromised.

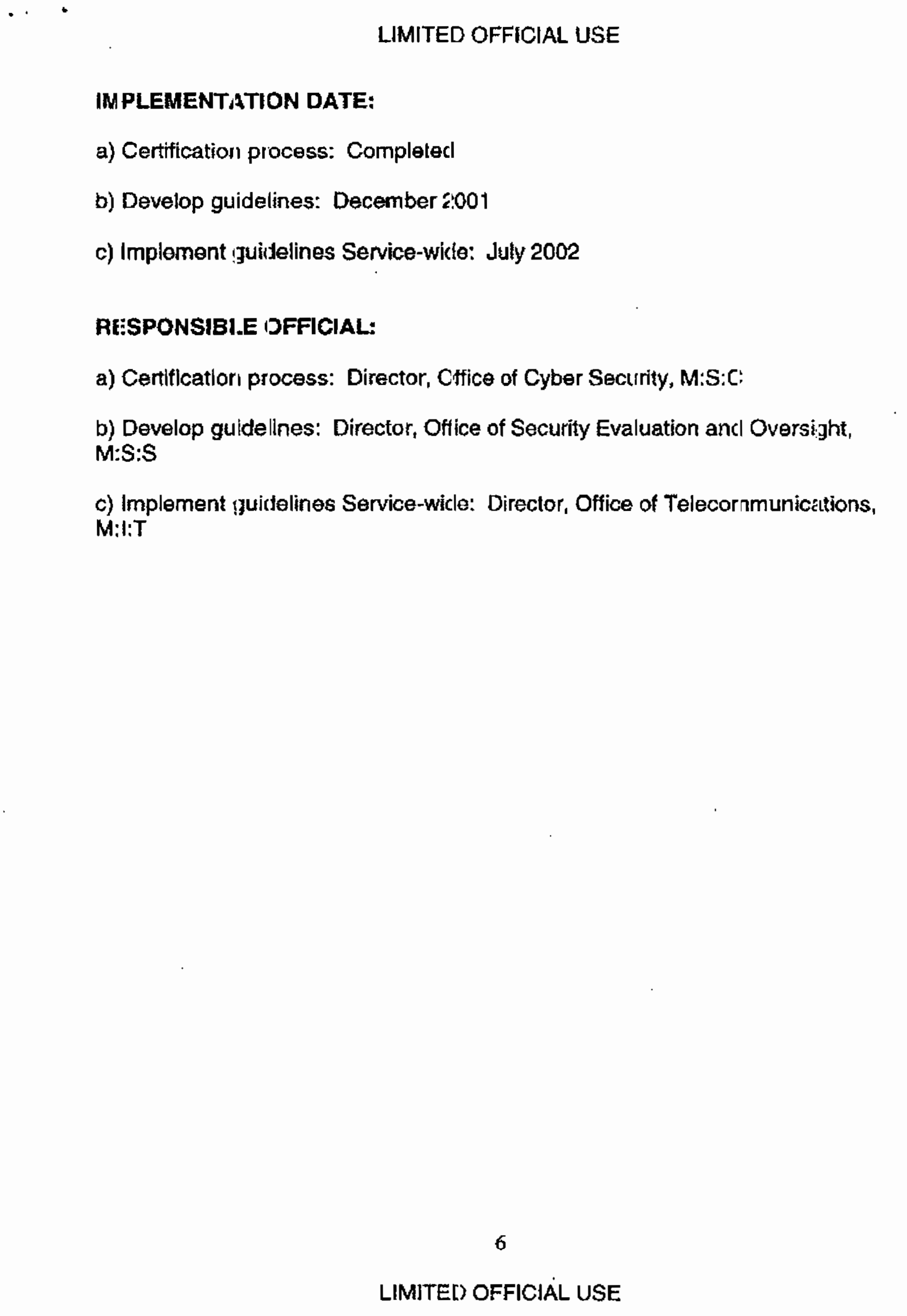
CORRECTIVE ACTION TO RECOMMENDATION #5:

We are taking corrective actions to address this recommendation. We have completed some processes and are developing others. Specifically:

a) Owners of all applications and systems that process, transmit, or store sensitive but unclassified information must have a risk assessment and security plan in place (and updated at least every three years) before they receive a security certification. In these documents, we identified data sensitivity analysis and requisite risk mitigation requirements as well as any point-to-point encryption requirement.

b) The Office of Security Evaluation and Oversight (SEO) conducted vulnerability assessments showing we need additional controls to manage network diagnostic tools. SEO is developing operations security guidelines, standards and procedures governing the use of data scopes (sniffers/analyzers) and network scanning tools.

c) The Office of Telecommunications will implement and enforce the guidelines.



LIMITED OFFICIAL USE

IMPLEMENTATION DATE:

a) Certification process: Completed

b) Develop guidelines: December 2001

c) Implement guidelines Service-wide: July 2002

RESPONSIBLE OFFICIAL:

a) Certification process: Director, Office of Cyber Security, M:S:C

b) Develop guidelines: Director, Office of Security Evaluation and Oversight, M:S:S

c) Implement guidelines Service-wide: Director, Office of Telecommunications, M:I:T

LIMITED OFFICIAL USE

RECOMMENDATION #6a:

The Deputy Commissioner for Modernization & CIO should establish realistic commitments to phase out current DES technology. This phase out should include the final dissolution of the first shared Treasury network circuitry and destruction of the associated DES encryption equipment.

ASSESSMENT OF CAUSE:

Although the IRS has migrated its applications off of the earlier version of the Treasury network, other Treasury bureaus still use the network and depend on equipment in IRS facilities.

CORRECTIVE ACTION TO RECOMMENDATION #6a:

We are taking actions to correct this weakness. The Office of Telecommunications is establishing commitments with the Treasury and other bureaus to phase out current DES technology. This phase out will include the final dissolution of the first shared Treasury network circuitry and destruction of the associated DES encryption equipment.

IMPLEMENTATION DATE:

July 2003

RESPONSIBLE OFFICIAL:

Director, Office of Telecommunications, M:I:T

RECOMMENDATION #6b:

The Deputy Commissioner for Modernization & CIO should establish realistic commitments to phase out current DES technology. This phase out should include the migration of the major segment of mainframe communications between computing centers and service centers from the current dedicated circuits that employ DES encryption to a Triple DES solution.

ASSESSMENT OF CAUSE:

The NIST FIPS-PUB 46-3 encourages government agencies still employing DES systems to transition to Triple DES encryption devices and directs them to implement Triple DES devices for new development. Although the NIST did not establish a due date for replacing the DES system, the advances in technology since 1998 and the rapidly decreasing costs for information technology warrant a plan that specifies when we can expect replacement.

CORRECTIVE ACTION TO RECOMMENDATION #6b:

We are taking actions to correct this weakness. The Office of Telecommunications is establishing commitments to phase out current DES technology. This will include migrating the major segment of mainframe communications between computing centers and service centers from the current dedicated circuits that employ DES encryption to a Triple DES solution.

IMPLEMENTATION DATE:

June 2002

RESPONSIBLE OFFICIAL:

Director, Office of Telecommunications, M:I:T