

**Certifying the Security of  
Internal Revenue Service Computer  
Systems Is Still A Material Weakness**

**June 2000**

**Reference Number: 2000-20-092**

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



DEPARTMENT OF THE TREASURY  
WASHINGTON, D.C. 20220

INSPECTOR GENERAL  
for TAX  
ADMINISTRATION

June 14, 2000

MEMORANDUM FOR COMMISSIONER ROSSOTTI

A handwritten signature in cursive script that reads "Pamela J. Gardiner".

FROM: Pamela J. Gardiner  
Deputy Inspector General for Audit

SUBJECT: Final Audit Report - Certifying the Security of Internal Revenue  
Service Computer Systems Is Still a Material Weakness

This report presents the results of our review of certifying and accrediting the security of the Internal Revenue Service's (IRS) computer systems. In summary, we found that almost 90 percent of the IRS' information systems are still not certified and accredited. Certifying the security of sensitive systems has been classified as a material control weakness since 1997. Furthermore, we are aware of only one IRS information system currently in use that had been certified and accredited before it was initially implemented. We believe that the IRS should expedite its ongoing efforts to certify systems already in use and avoid deploying new systems until they are certified and accredited.

We estimate that the IRS will pay contractors \$26 million to develop security documentation for systems that were rolled out without the necessary security controls. Most of this cost could have been avoided if security controls had been built in and certification and accreditation had been accomplished during systems development.

Management agreed to the recommendations presented. Management's comments have been incorporated into the report where appropriate, and the full text of their comments is included as an appendix.

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 your staff may call Scott E. Wilson, Associate Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

**Certifying the Security of Internal Revenue Service  
Computer Systems Is Still A Material Weakness**

---

**Table of Contents**

Executive Summary.....	Page i
Objective and Scope.....	Page 1
Background .....	Page 2
Results .....	Page 3
The Majority of the Internal Revenue Service's Information Systems Were Not Certified and Accredited as Required.....	Page 4
The Certification Program Office Does Not Have Sufficient Information to Monitor Accreditations .....	Page 9
Conclusion.....	Page 10
Appendix I – Detailed Objective, Scope, and Methodology .....	Page 11
Appendix II – Major Contributors to This Report.....	Page 14
Appendix III – Report Distribution List.....	Page 15
Appendix IV – Outcome Measures.....	Page 16
Appendix V – Management’s Response to the Draft Report .....	Page 18

## **Certifying the Security of Internal Revenue Service Computer Systems Is Still A Material Weakness**

---

### **Executive Summary**

Office of Management and Budget and Treasury Department directives require that all information systems that process sensitive but unclassified information, including taxpayer data, be certified and accredited prior to being placed into operation. In addition, these information systems are required to be re-certified and re-accredited at least every three years or when significant modifications occur. Certifying that adequate security controls have been developed and accrediting that the risks of security breaches have been adequately reduced are the two primary controls for ensuring that security controls are built into new information systems and remain up-to-date afterwards. At stake is the privacy of information for over 123 million taxpayers.

The Certification Program Office, under the direction of the Office of Security and Privacy Oversight, is responsible for certifying that Internal Revenue Service (IRS) information systems have sufficient security controls. The IRS executive in charge of the function using each information system is responsible for accrediting the system. When accrediting, executives state that they are aware of and accept the risks associated with operating the system.

In 1995, the IRS began monitoring sensitive systems certification as a potential management control weakness and in 1997 officially reported it as a material weakness. This issue continues to be an open item on its Fiscal Year 1999 assessment of management controls.

The overall objective of this audit was to assess the effectiveness of the IRS' security certification and accreditation processes for information systems and networks.

### **Results**

The majority of IRS information systems are still not certified and accredited. Although the IRS is taking steps through contractor support to alleviate this situation, more emphasis is needed to resolve this material control weakness in a timely manner.

### **The Majority of the Internal Revenue Service's Information Systems Were Not Certified and Accredited as Required**

Of the 258 systems listed on the inventory of sensitive systems in January 2000, 232 (89.9 percent) were not certified. Responsible executives had granted temporary authorities to operate 143 of the uncertified systems but had accepted no accountability for the security risks of operating the other 89 systems.

## **Certifying the Security of Internal Revenue Service Computer Systems Is Still A Material Weakness**

---

We attribute these conditions in part to the lack of emphasis the IRS has placed on building security controls into new information systems. It has become a standard practice in the IRS to implement a system without the necessary certification and accreditation of security controls. We are aware of only one information system currently in use that had been certified and accredited before it was initially implemented.

Documenting security controls for the uncertified systems after they have been implemented will cost the IRS about \$26 million. This cost could have been greatly reduced if security controls had been built in and certification and accreditation had been accomplished during systems development.

### **The Certification Program Office Does Not Have Sufficient Information to Monitor Accreditations**

IRS guidelines require that the Certification Program Office provide timely status and technical information regarding certification and accreditation of IRS information systems to responsible executives. However, there is no control in place within the certification program to ensure that accreditations are granted and granted timely for certified systems.

### **Summary of Recommendations**

The IRS should place more emphasis on building security controls into new information systems. To ensure this happens, IRS management should not authorize the implementation of any new system until controls are sufficient and the system has the required security certification and accreditation.

For systems that are already implemented, the IRS needs to place additional emphasis on timely certification and accreditation. The IRS should ensure that funds continue to be allocated for contractor support during the certification process and consideration should be given to increasing this allocation in order to get systems certified as soon as possible. Consideration should also be given to increasing the human resources within the IRS devoted to certifying and accrediting the security features of systems.

Also, the process for identifying all information systems requiring certification and accreditation, and the tracking of their certification and accreditation status, should be centralized.

Management's Response: Management generally agreed with our findings and recommendations. They are developing a new process for certifying new systems within the systems development life cycle. Management anticipates that systems will be implemented without full certification only in special circumstances. Contractor support

## **Certifying the Security of Internal Revenue Service Computer Systems Is Still A Material Weakness**

---

will continue to be used to reduce the backlog of uncertified systems. Management's complete response to the draft report is included as Appendix V.

Office of Audit Comment: We believe that management's response is adequate with one important exception. Considering the sensitivity of the data processed by the IRS and the risks inherent in today's interconnected computer systems, we do not believe that any new system should be implemented without appropriate security controls.

## Certifying the Security of Internal Revenue Service Computer Systems Is Still A Material Weakness

---

### Objective and Scope

*The objective of this audit was to determine whether the IRS' security certification process for information systems and networks is effective.*

The overall objective of this audit was to determine whether the Internal Revenue Service's (IRS) security certification process for information systems and networks is effective. Specifically, we:

- Determined whether information systems in use were certified and re-certified when appropriate.
- Determined whether information systems in use were accredited and re-accredited when appropriate.

To accomplish our objective, we reviewed guidelines and procedures relevant to the certification of security controls in IRS information systems, interviewed IRS personnel responsible for certifying that IRS information systems have sufficient security controls, and reviewed supporting documentation relating to the certification of IRS information systems. In addition, we contacted representatives for 235 of the 258 systems on the Certification Program Office's inventory of sensitive systems as of January 13, 2000, to obtain information relevant to the certification and accreditation of their systems.

The scope of this audit did not include determining the adequacy or completeness of individual security certifications and accreditations or supporting documentation. The scope was limited to determining if the process in place for certifying and accrediting IRS information systems was effective in ensuring that all systems in use are timely certified and accredited.

This audit was conducted in the National Office between December 1999 and February 2000, in accordance with *Government Auditing Standards*. Details of our audit objective, scope, and methodology are presented in Appendix I. Major contributors to this report are listed in Appendix II.

## Certifying the Security of Internal Revenue Service Computer Systems Is Still A Material Weakness

---

### Background

*OMB and Treasury Department directives require that information systems be certified and accredited prior to being placed into operation.*

The Office of Management and Budget (OMB) Circular A-130 and the Department of the Treasury Security Manual require that all information systems that process sensitive but unclassified information, including taxpayer data, be certified and accredited prior to being placed into operation. In addition, these information systems are required to be re-certified and re-accredited at least every three years or when significant modifications occur.

Certification and accreditation are the two primary controls for ensuring that security controls are built into new information systems before they are implemented and that security controls remain up-to-date afterwards.

- Certification requires a comprehensive evaluation of technical and non-technical security features to determine the extent to which system design and implementation meet a specified set of security requirements.
- Accreditation is the issuance of an official declaration by the responsible official that an information system or network is approved to operate with prescribed security safeguards.

*The Certification Program Office is responsible for the security certification process for IRS information systems.*

The Certification Program Office, under the direction of the Office of Security and Privacy Oversight, is responsible for the security certification process for IRS information systems. IRS functional executives are responsible for the accreditation of IRS information systems.



## Certifying the Security of Internal Revenue Service Computer Systems Is Still A Material Weakness

---

*Sensitive systems certification has been identified as a material weakness in the IRS' management controls since 1997.*

The Federal Managers' Financial Integrity Act (FMFIA)<sup>1</sup> requires each federal agency to conduct an annual self-assessment of its management controls and to report any weaknesses in these controls along with plans for corrective action. In 1995, the IRS began monitoring sensitive systems certification as a potential management control weakness and in 1997 officially reported it as a material weakness in its management controls. This issue continues to be an open item on the IRS' Fiscal Year 1999 assessment of management controls.

### Results

*The majority of IRS information systems are not certified and accredited.*

Almost 90 percent of IRS information systems have not been granted current security certifications and accreditations. We are aware of only one system currently in use that had been certified and accredited before it was initially implemented.

Furthermore, there is no process or control in place to ensure that certified systems are accredited. In addition, information and related documentation for those systems that are actually accredited is not readily available.

*More emphasis is needed to resolve this material control weakness in a timely manner.*

Although the IRS is taking steps through contractor support during the certification process to get its information systems certified, more emphasis is needed to resolve this material control weakness in a more timely manner. At stake is the privacy of data for over 123 million taxpayers.

---

<sup>1</sup> Federal Managers' Financial Integrity Act of 1982, 31 U.S.C. §§ 1105-1106, 1113, and 3512 (1994)

## Certifying the Security of Internal Revenue Service Computer Systems Is Still A Material Weakness

---

### **The Majority of the Internal Revenue Service's Information Systems Were Not Certified and Accredited as Required**

---

---

*Only 26 (10.1 percent) of the 258 systems on the inventory of sensitive systems were certified.*

Of the 258 sensitive systems identified on the Certification Program Office's inventory as of January 2000, 232 (89.9 percent) were not certified. Of the 232 systems not certified, 29 had prior certifications and accreditations that had expired or had been revoked due to significant modifications. The other 203 systems had never been certified.

Responsible executives had granted temporary authority to operate 143 of the 232 non-certified systems while awaiting final certification and accreditation. Essentially, they had assumed responsibility for the risk associated with operating these systems. However, they had assumed no responsibility for operating the other 89 systems.

*Not all IRS systems are inventoried. Those not on the inventory are not certified and accredited.*

Additional sensitive systems were not identified on the Certification Program Office's inventory and, accordingly, were not certified or accredited. One executive recently advised the Certification Program Office that 95 existing systems should be added to the inventory and scheduled for certification. Some of these systems had been in operation for over 13 years.

*The IRS does not have adequate assurance that all taxpayer data is secure.*

The privacy of taxpayer information is at greater risk of being breached when IRS information systems have not been certified and accredited. The IRS does not have adequate assurance that personal data for millions of taxpayers is secure.

We attribute these conditions to the following:

- Lack of emphasis on building security into new systems.
- Lack of resources devoted to the certification program.

## Certifying the Security of Internal Revenue Service Computer Systems Is Still A Material Weakness

---

- Lack of coordination between functional executives and the Certification Program Office.

*We are aware of only one information system currently in use that had been certified and accredited before it was initially implemented.*

*Documenting security controls is currently costing the IRS \$111,000 per system.*

### **Lack of emphasis on building security into new systems**

One of the contributing factors to information systems not being certified was the lack of emphasis the IRS has placed on building security controls into new information systems. We are aware of only one information system currently in use that had received a security certification and accreditation before being initially implemented.

The lack of emphasis on building security controls into new information systems and obtaining the required certification and accreditation prior to implementation has contributed to the significant backlog of non-certified systems. In addition, documenting security controls for systems after they have been implemented is currently costing the IRS an average of \$111,000 per system. We estimate the cost of documenting the 232 non-certified systems to be approximately \$26 million. This cost could have been greatly reduced if security controls had been built in and certification and accreditation had been accomplished during systems development.

To roll out the system quickly, the accrediting executive may request approval to grant an Interim Authority to Operate (IAO) to authorize the implementation pending final certification. An IAO provides up to an additional year to obtain certification, but it gives only minimal assurance that security controls are effective.

IAOs were issued for new systems and, in at least 12 instances, systems had been granted multiple IAOs. This practice has enabled executives responsible for developing new systems to roll out systems without placing sufficient emphasis on building in the necessary security controls. Once a new system is implemented with an IAO, it is unlikely the IRS would shut it down, even when the IAO expired.

## Certifying the Security of Internal Revenue Service Computer Systems Is Still A Material Weakness

---

*Limited resources are available to the Certification Program Office.*

### **Lack of resources devoted to the certification program**

Another contributing factor for systems on the inventory not being certified was that the Certification Program Office had limited resources. In October 1999, the 7 analysts in the Certification Program Office were each assigned over 25 systems for which they were responsible for providing certification support. These workloads also prevented the Certification Program Office personnel from performing appropriate follow-ups.

*The Certification Program Office relies on the systems' users to advise it of the existence of IRS information systems requiring certification.*

### **Lack of coordination between functional executives and the Certification Program Office**

The primary reason that all sensitive systems were not included on the inventory is that users did not advise the Certification Program Office that the system existed. Users are required to submit a Request for Certification Support to the Certification Program Office to advise it of their system and request support. Input as to the completeness of the inventory is requested once each year as part of the FMFIA assurance process.

*The IRS is taking steps to improve the certification process and to alleviate the backlog of non-certified systems.*

The IRS is taking steps to improve the certification process and to alleviate the backlog of non-certified systems. For example,

- The IRS is working with a contractor to build security, including testing and certification, into the software development process. This will help to ensure that information systems are certified and accredited during development and prior to implementation.
- In order to get existing systems certified, the IRS has begun using contractor support during the certification process to evaluate security features and to prepare required certification documentation.

## **Certifying the Security of Internal Revenue Service Computer Systems Is Still A Material Weakness**

---

Although the IRS is taking some steps to improve the certification process, more emphasis is needed to resolve this material control weakness in a timely manner.

### **Recommendations**

1. Information Systems management should place more emphasis on building security controls into new information systems. To ensure this happens, IRS management should not authorize the implementation of any new system until controls are sufficient and the system has the required security certification and accreditation. IAOs should not be issued for new systems.
2. For systems that have already been implemented, Information Systems management needs to place additional emphasis on timely certification and accreditation. Information Systems management should ensure that funds continue to be allocated for contractor support during the certification process and consideration should be given to increasing this allocation in order to get systems certified as soon as possible.
3. Information Systems management should consider increasing the human resources within the IRS devoted to certifying and accrediting the security features of information systems.
4. Information Systems management should ensure that the IRS' certification process includes follow-ups with the accrediting executives prior to the expiration of their systems security certification to ensure that they are aware that a new certification and accreditation is required.
5. Information Systems management should ensure that all functional executives for individual systems are fully aware of the overall certification and accreditation process.

## **Certifying the Security of Internal Revenue Service Computer Systems Is Still A Material Weakness**

---

6. Information Systems management should centralize the process for identifying and tracking of all information systems requiring certification and accreditation. Once the process is centralized, an effort should be made to identify all existing information systems requiring certification and accreditation. New information systems should be identified during development to ensure that certification and accreditation is accomplished prior to implementation.

Management's Response: The Office of Security and Privacy Oversight has an initiative underway to improve the certification and accreditation process. The process will include assessing new systems early in the development life cycle to ensure that requirements are known and adequately addressed. Systems will be implemented without full certification on a very limited basis. Other components of the process include reducing the backlog of uncertified systems with contractor support, coordinating more effectively with accrediting executives, and tracking the progress of systems during development to ensure that actions are taken to certify the system before implementation.

Office of Audit Comment: We believe that management's response is adequate with one important exception. Considering the sensitivity of the data processed by the IRS and the risks inherent in today's interconnected computer systems, we do not believe that any new system should be implemented without appropriate security controls.

## Certifying the Security of Internal Revenue Service Computer Systems Is Still A Material Weakness

---

### The Certification Program Office Does Not Have Sufficient Information to Monitor Accreditations

*One of the Certification Program Office's responsibilities is to provide timely information on certification and accreditation of IRS information systems.*

One of the Certification Program Office's responsibilities is to provide timely status and technical information regarding certification and accreditation of IRS information systems to responsible executives. As previously mentioned, only 26 of the 258 systems listed on the inventory of sensitive systems were certified. However, the Certification Program Office had information on only 5 of the 26 certified systems indicating that they had been accredited. There is no control in place within the IRS' certification process to ensure that accreditations are granted and granted timely for certified systems. As a result, systems were placed into production without any IRS official accepting accountability for security.

*The Certification Program Office has no accreditation information available for the majority of certified systems.*

Although the Certification Program Office does request a copy of the official accreditation in the transmittal accompanying the certification statement, it seldom receives a copy. In addition, the Certification Program Office does not follow-up after certification of a system to see if an accreditation was actually issued.

The Certification Program Office had a copy of the official IAO issued by the accrediting executive for only 6 of the 143 systems shown on the inventory as having an IAO as of January 13, 2000. The Certification Program Office does not request a copy of the official IAO from the responsible executive.

*The actual IAO issue and/or expiration dates were different than those maintained by the Certification Program Office in 82.4 percent of the cases.*

The IAO issue date and expiration date maintained by the Certification Program Office were often inaccurate. We reviewed IAOs for 125 of the 143 systems which had been granted an IAO. The issue and/or expiration dates maintained by the Certification Program Office were inaccurate for 103 (82.4 percent) of the 125 documents. Since the Certification Program Office generally does not have a copy of the official IAO, it

## **Certifying the Security of Internal Revenue Service Computer Systems Is Still A Material Weakness**

---

determined the expiration date by adding one year to the date it notified the functional executive that an IAO was approved. However, the accrediting executive can issue the IAO for any period of time up to, but not to exceed, one year.

### **Recommendation**

7. Information Systems management should ensure that the IRS' certification process includes follow-ups with the accrediting executives to ensure that necessary information relevant to the official accreditation is provided and to educate them on the importance of providing this information. Once obtained, information relevant to the official accreditation should be maintained and tracked in a centralized location for reporting purposes.

Management's Response: The Office of Security and Privacy Oversight's new certification process will include the capability to track the accreditation status, post-implementation review status, and any deviations from the certification process.

### **Conclusion**

*The majority of IRS information systems are not certified and accredited.*

The IRS certification and accreditation processes have not been effective in ensuring that security is built into new information systems. Once a system is rolled out, it is often difficult and expensive to add those controls. The IRS is taking steps through contractor support during the certification process to alleviate this situation. However, more emphasis is needed to resolve this material control weakness in a timely manner to reduce costs and better protect the privacy of taxpayers' information.



## Certifying the Security of Internal Revenue Service Computer Systems Is Still A Material Weakness

---

### Appendix I

#### Detailed Objective, Scope, and Methodology

The overall objective of this audit was to determine whether the Internal Revenue Service's (IRS) security certification process for information systems and networks is effective. Specifically, we:

- Determined whether information systems in use were certified and re-certified when appropriate.
- Determined whether information systems in use were accredited and re-accredited when appropriate.

We conducted the following tests to accomplish the objective:

- I. Determined specific requirements of law, regulation, and standards for the IRS in terms of security certification and accreditation of its information systems and networks. Specifically, we:
  - A. Reviewed pertinent portions of Public Laws (e.g., Public Law 100-235, The Computer Security Act of 1987), the United States Code, and Federal Regulations.
  - B. Reviewed pertinent Office of Management and Budget (OMB) Circulars (e.g., No. A-127, No. A-130, etc.).
  - C. Reviewed *Guidelines for Computer Security Certification and Accreditation* (Federal Information Processing Standards Publication 102).
  - D. Reviewed National Computer Security Center, *Introduction to Certification and Accreditation* (NCSC-TG-029).
- II. Reviewed written policies and procedures in place within the IRS and the Department of the Treasury relative to the security certification and accreditation of IRS information systems and networks.
- III. Determined the processes, procedures, and controls used by the IRS to ensure that its information systems and networks are certified and accredited when appropriate. Specifically, we:

## **Certifying the Security of Internal Revenue Service Computer Systems Is Still A Material Weakness**

---

- A. Performed a walk-through of the Certification Program Office in the National Office to determine the processes and procedures in place for certifying and re-certifying IRS information systems and networks.
- B. Interviewed National Office personnel in the Certification Program Office to:
  - 1. Determine their perspective on the average time it takes to certify and accredit an information system and a network.
  - 2. Obtain their current inventory of systems and/or networks requiring security certification, including the status of the security certification and accreditation for each system and/or network.
  - 3. Request access to their security certification and/or accreditation files for all IRS information systems and networks.
- IV. Determined if current security certifications and accreditations existed for each system and network identified in III above. For the information systems and/or networks that did not have a current security certification or accreditation, we determined the cause, whether interim authorities to operate had been granted, and if they were appropriate.
- V. For all information systems and networks that did have a current accreditation as determined in IV above, we determined if the accreditation was appropriate. Specifically, we:
  - A. Determined if a security certification was completed prior to the accreditation.
  - B. For those with a security certification prior to accreditation, we determined if the security certification packages were complete<sup>1</sup>, per Internal Revenue Manual 2.1.10.2.3.5, including:
    - Risk Assessment
    - Computer Security Plan
    - System Notice
    - Configuration Management documentation
    - Continuity Of Operations Plan
    - Trusted Facility Manual
    - Security Features User's Guide
    - Security Test and Evaluation (STE) Report

---

<sup>1</sup> We did not evaluate the adequacy of these documents, but only determined if they existed.

**Certifying the Security of Internal Revenue Service  
Computer Systems Is Still A Material Weakness**

---

- Privacy Impact Assessment
  - Any exceptions from the C2 requirements
- C. Determined if the accreditation package was complete.
- D. Determined if the appropriate level IRS executive was selected as the accrediting authority.

**Certifying the Security of Internal Revenue Service  
Computer Systems Is Still A Material Weakness**

---

**Appendix II**

**Major Contributors to This Report**

Scott E. Wilson, Associate Inspector General for Audit (Information Systems Programs)  
Stephen R. Mullins, Director  
Joseph C. Wabnitz, Audit Manager  
Cecil A. Begley, Senior Auditor  
Richard J. Flynn, Senior Auditor  
John W. Baxter, Auditor  
Carol A. Rowland, Auditor  
Una K. Smith, Auditor  
Marjorie Stephenson, Auditor

**Certifying the Security of Internal Revenue Service  
Computer Systems Is Still A Material Weakness**

---

**Appendix III**

**Report Distribution List**

Chief Information Officer IS  
Director, Office of Security and Privacy Oversight IS:SPO  
Director, Security, Evaluation and Oversight IS:SPO:S  
Director, Office of Program Evaluation and Risk Analysis M:O  
National Director for Legislative Affairs CL:LA  
Office of Management Controls M:CFO:A:M  
Office of Chief Counsel CC  
Office of the National Taxpayer Advocate C:TA  
Audit Liaison  
    Chief Information Officer IS

## Certifying the Security of Internal Revenue Service Computer Systems Is Still A Material Weakness

---

### Appendix IV

#### Outcome Measures

This appendix presents detailed information on the measurable impact that our recommended corrective actions will have on tax administration. These benefits will be incorporated into our Semiannual Report to the Congress.

Finding and recommendation:

The majority of Internal Revenue Service (IRS) information systems were not certified and accredited as required. Of the 258 systems identified on the Certification Program Office's inventory of sensitive systems as of January 13, 2000, only 26 (10.1 percent) were certified. The remaining 232 (89.9 percent) were not certified. For the many taxpayers who have information on these 232 non-certified systems, the IRS does not have adequate assurance that the data is secure since the information systems do not have the proper security certification and accreditation.

The IRS should place more emphasis on building security controls into new information systems. To ensure this happens, IRS management should not authorize the implementation of any new system until controls are sufficient and the system has the required security certification and accreditation. Interim Authorities to Operate should not be issued on any new system.

For systems that have already been implemented, the IRS needs to place additional emphasis on timely security certification and accreditation. The IRS should ensure that funds continue to be allocated for contractor support during the certification process and consideration should be given to increasing this allocation in order to get systems certified as soon as possible. In addition, consideration should be given to increasing the human resources available to the certification program.

Type of Outcome Measure:

The security certification and accreditation process is a critical part of the IRS' overall computer security initiative. Thus, potential outcomes can be expected for the following measures:

- Taxpayer privacy and security.
- Protection of resources/reliability of information.

## **Certifying the Security of Internal Revenue Service Computer Systems Is Still A Material Weakness**

---

### Value of the Benefit:

Obtaining the required security certification and accreditation for each of the non-certified IRS information systems would provide greater assurance that the data for the 123 million taxpayers is secure and reliable.

### Methodology Used to Measure the Reported Benefit:

The IRS Statistics of Income Division estimates over 123 million taxpayers filed tax returns in 1998, the most current year statistics are readily available. Since all taxpayer data is located on one or more of the IRS' information systems, the security of the data for all taxpayers is relevant to this audit.

In addition, the IRS is currently paying contractors about \$111,000 per system to document security controls. To pay a contractor at this rate to document the 232 uncertified systems could cost the IRS nearly \$26 million. Since this amount will have to be spent regardless of our recommendations, we are not considering it an outcome measure but consider it an impact of placing systems into production without certifying security.

By building security controls into new systems in accordance with a security architecture, the IRS would only have to document and certify compliance with the architecture and ensure exceptions to the architecture were reasonably secure. No data exist to estimate this cost, but we believe the cost would be minimal and the work could possibly be done with current project personnel. To compute the cost that could have been avoided, we did not consider the cost of certifying the system. The IRS is currently paying contractors about \$27,000 per system for testing and certifying. While some of this cost would be incurred regardless of when security controls were designed, we believe a significant amount could be avoided if systems were designed to meet a security architecture.

**Certifying the Security of Internal Revenue Service  
Computer Systems Is Still A Material Weakness**

**Appendix V**

**Management's Response to the Draft Report**




COMMISSIONER

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

June 2, 2000

MEMORANDUM FOR TREASURY INSPECTOR GENERAL FOR TAX  
ADMINISTRATION

FROM:

Charles O. Rossotti   
Commissioner of Internal Revenue

SUBJECT:

Response to Draft Audit Report – Certifying the Security of  
Internal Revenue Service Computer Systems is Still a Material  
Weakness (Audit No. 199920107)

Thank you for the opportunity to review and comment on your draft report and its recommendations for improving the Internal Revenue Service's (IRS) systems security certification and accreditation program. While we generally agree with your findings, we cannot commit to expending additional resources as recommended at this time, without completing our ongoing evaluation to identify a more efficient, effective, and responsible approach to systems certification.

The IRS has focused considerable resources and efforts over the last few years to improve its security infrastructure and processes. In 1997, we established a Security and Privacy Oversight Office, which has worked with other IRS offices to achieve measurable security improvements. One of our ongoing initiatives is focused on improving the certification and accreditation process. An important goal of the new process will be to establish a more efficient and effective approach, which focuses on certifying new systems within the systems development life cycle to ensure that security requirements are adequately designed, developed, tested, and implemented. Simultaneously, we are continuing to make significant funding commitments by using contractor support to help reduce our large backlog of uncertified systems. We are currently evaluating how to improve the certification and accreditation process to better address this backlog. Attached are detailed responses to each of your report's recommendations.

If you have any questions, please contact Paul Cosgrave, Chief Information Officer, at (202) 622-6800 or have a member of your staff contact Len Baptiste, Director, Office of Security and Privacy Oversight at (202) 622-8910.

Attachment



## **Certifying the Security of Internal Revenue Service Computer Systems Is Still A Material Weakness**

### **Management Response to Draft Audit Report – Certifying the Security of Internal Revenue Service Computer Systems is Still a Material Weakness**

#### Recommendation #1

Information Systems management should place more emphasis on building security controls into new information systems. To ensure this happens, IRS management should not authorize the implementation of any new system until controls are sufficient and the system has the required security certification and accreditation. Interim Authority to Operate (IAOs) should not be issued for new systems.

#### Assessment of Cause

Lack of emphasis on building security into new systems.

#### Corrective Action #1

The Office of Security and Privacy Oversight has an initiative underway to improve the current certification and accreditation process. A key component of this process will be to certify all new systems. This approach will include assessing new systems early in the systems development life cycle to ensure that security requirements are known and adequately addressed. We are in the process of implementing more stringent controls to ensure that interim authorities to operate (IAO) for new systems will only be used when special circumstances warrant them. We are anticipating granting IAO's for new systems on a very limited, highly exceptional basis.

#### Implementation Date of Corrective Action #1

Completed: Proposed: April 30, 2001

#### Responsible Officials for Corrective Action #1

Chief Information Officer IS  
Director, Security and Privacy Oversight IS:SPO  
Business Systems Modernization Executive

#### Corrective Action #1 Monitoring Plan

The Office of Security and Privacy Oversight is establishing clear goals, objectives, milestones, and measures. Project management techniques and tools will be used to plan, control, and track the task, resources, and schedules.

## **Certifying the Security of Internal Revenue Service Computer Systems Is Still A Material Weakness**

### **Management Response to Draft Audit Report – Certifying the Security of Internal Revenue Service Computer Systems is Still a Material Weakness**

#### Recommendation #2

For systems that have already been implemented, Information Systems management needs to place additional emphasis on timely certification and accreditation. Information Systems management should ensure that funds continue to be allocated for contractor support during the certification process and consideration should be given to increasing this allocation in order to get systems certified as soon as possible.

#### Assessment of Cause

Documenting security controls for systems after they have been implemented is currently costing the IRS an average \$111,000 per system. This cost could have been reduced if security controls had been built in and certification and accreditation had been accomplished during development.

#### Corrective Action #2

The Office of Security and Privacy Oversight is currently evaluating how to improve the certification and accreditation process. A key component of this process is to establish a better approach to address the backlog of over 200 uncertified systems. We plan to establish a risk-based, workable approach to ensure that we do not spend our limited resources on older or low-risk systems where the risk would not justify the cost to complete the certification.

#### Implementation Date of Corrective Action #2

Completed:                                  Proposed: December 29, 2000

#### Responsible Officials for Corrective Action #2

Chief Information Officer IS  
Director, Security and Privacy Oversight IS:SPO

#### Corrective Action #2 Monitoring Plan

The Office of Security and Privacy Oversight is establishing clear goals, objectives, milestones, and measures. Project management techniques and tools will be used to plan, control, and track the task, resources, and schedules. We will conduct a pilot to validate that the goals of improving the certification and accreditation process and certifying the backlog of over 200 systems were achieved.

## **Certifying the Security of Internal Revenue Service Computer Systems Is Still A Material Weakness**

### **Management Response to Draft Audit Report – Certifying the Security of Internal Revenue Service Computer Systems is Still a Material Weakness**

#### Recommendation #3

Information Systems management should consider increasing the human resources within the IRS devoted to certifying and accrediting the security features of information systems.

#### Assessment of Cause

In October 1999, the 7 analysts in the Certification Program Office were each assigned over 25 systems for which they were responsible for providing certification support. These workloads were too high and prevented the Certification Program Office from performing appropriate follow-ups.

#### Corrective Action #3

The Office of Security and Privacy Oversight is currently evaluating how to improve the certification and accreditation process. Key components of this process include establishing an approach to better address the backlog of over 200 uncertified systems and integrating the security certification process into the IRS' Enterprise Life Cycle (the modernized business systems life cycle methodology). This integration will reduce the workload of Certification Program Office resources and allow them to focus on tracking, monitoring, and follow-ups.

#### Implementation Date of Corrective Action #3

Completed:                      Proposed: April 30, 2001

#### Responsible Officials for Corrective Action #3

Chief Information Officer IS  
Director, Security and Privacy Oversight IS:SPO

#### Corrective Action #3 Monitoring Plan

The Office of Security and Privacy Oversight is establishing clear goals, objectives, milestones, and measures. Project management techniques and tools will be used to plan, control and track the task, resources, and schedules. We will conduct a pilot to validate that the goals of improving the certification and accreditation process and certifying the backlog of over 200 systems were achieved.

## **Certifying the Security of Internal Revenue Service Computer Systems Is Still A Material Weakness**

### **Management Response to Draft Audit Report – Certifying the Security of Internal Revenue Service Computer Systems is Still a Material Weakness**

#### Recommendation #4

Information Systems management should ensure that the IRS' certification process includes follow-ups with the accrediting executives prior to the expiration of their systems security certification to ensure they are aware that a new certification and accreditation is required.

#### Assessment of Cause

Excessive workloads prevented the Certification Program Office from performing appropriate follow-ups to previously accredited systems.

#### Corrective Action #4

The Office of Security and Privacy Oversight is assessing and improving the current certification and accreditation process. A key component of this process will include follow-ups prior to the expiration of a system's security certification to ensure that individuals responsible for the recertification are aware of this requirement.

#### Implementation Date of Corrective Action #4

Completed:                      Proposed: April 30, 2001

#### Responsible Officials for Corrective Action #4

Chief Information Officer IS  
Director, Security and Privacy Oversight IS:SPO

#### Corrective Action #4 Monitoring Plan

The Office of Security and Privacy Oversight is establishing clear goals, objectives, milestones, and measures. Project management techniques and tools will be used to plan, control and track the task, resources, and schedules. We will conduct a pilot to validate that the goal of improving the certification and accreditation process was achieved.

## **Certifying the Security of Internal Revenue Service Computer Systems Is Still A Material Weakness**

### **Management Response to Draft Audit Report – Certifying the Security of Internal Revenue Service Computer Systems is Still a Material Weakness**

#### Recommendation #5

Information Systems management should ensure that all functional executives for individual systems are fully aware of the overall certification and accreditation process.

#### Assessment of Cause

The primary reason that all sensitive systems were not included on the inventory is that users and functional executives did not advise the Certification Program Office that the system existed.

#### Corrective Action #5

The Office of Security and Privacy Oversight is assessing and improving the current certification and accreditation process. A key component of this process will include communicating the requirements for obtaining certification and accreditation to IRS executives.

#### Implementation Date of Corrective Action #5

Completed:                      Proposed: April 30, 2001

#### Responsible Officials for Corrective Action #5

Chief Information Officer IS

Director, Security and Privacy Oversight IS:SPO

#### Corrective Action #5 Monitoring Plan

The Office of Security and Privacy Oversight is establishing clear goals, objectives, milestones, and measures. Project management techniques and tools will be used to plan, control, and track the tasks, resources, and schedules. We will conduct a pilot to validate that the goal of improving the certification and accreditation process was achieved.

## **Certifying the Security of Internal Revenue Service Computer Systems Is Still A Material Weakness**

### **Management Response to Draft Audit Report – Certifying the Security of Internal Revenue Service Computer Systems is Still a Material Weakness**

#### **Recommendation #6**

Information Systems management should centralize the process for identifying and tracking of all information systems requiring certification and accreditation. Once the process is centralized, an effort should be made to identify all existing information systems requiring certification and accreditation. New information systems should be identified during development to ensure that certification and accreditation is accomplished prior to implementation.

#### **Assessment of Cause**

The current centralized process lacks a mechanism to proactively identify systems requiring certification and accreditation. The current process also does not have a complete tracking and monitoring system.

#### **Corrective Action #6**

The Office of Security and Privacy Oversight is assessing and improving the current certification and accreditation process. A key component of this process will include improved tracking and monitoring capabilities, which will track a system's progress through the life cycle.

#### **Implementation Date of Corrective Action #6**

Completed:                      Proposed: April 30, 2001

#### **Responsible Officials for Corrective Action #6**

Chief Information Officer IS  
Director, Security and Privacy Oversight IS:SPO

#### **Corrective Action #6 Monitoring Plan**

The Office of Security and Privacy Oversight is establishing clear goals, objectives, milestones, and measures. Project management techniques and tools will be used to plan, control, and track the task, resources, and schedules. We will conduct a pilot to validate that the goal of improving the certification and accreditation process was achieved.

## **Certifying the Security of Internal Revenue Service Computer Systems Is Still A Material Weakness**

### **Management Response to Draft Audit Report – Certifying the Security of Internal Revenue Service Computer Systems is Still a Material Weakness**

#### Recommendation #7

Information Systems management should ensure that the IRS' certification process includes follow-ups with the accrediting executives to ensure that necessary information relevant to the official accreditation is provided and to educate them on the importance of providing this information. Once obtained, information relevant to the official accreditation should be maintained and tracked in a centralized location for reporting purposes.

#### Assessment of Cause

There are inadequate controls in place within the certification program to ensure that accreditations are granted and granted timely for certified systems.

#### Corrective Action #7

The Office of Security and Privacy Oversight is assessing and improving the current certification and accreditation process. A key component of this process will include a tracking capability that will keep executives apprised of their systems' certification progress through the systems development life cycle. In this regard, it will include the accreditation status, the post-implementation review status, and any deviations from the certification process.

#### Implementation Date of Corrective Action #7

Completed:                      Proposed: April 30, 2001

#### Responsible Officials for Corrective Action #7

Chief Information Officer IS  
Director, Security and Privacy Oversight IS:SPO

#### Corrective Action #7 Monitoring Plan

The Office of Security and Privacy Oversight is establishing clear goals, objectives, milestones, and measures. Project management techniques and tools will be used to plan, control, and track the task, resources, and schedules.