

**Although Still Behind in Certifying the  
Security of Sensitive Computer Systems,  
the Internal Revenue Service Has  
Made Significant Progress**

**September 2002**

**Reference Number: 2002-20-165**

**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

September 11, 2002

MEMORANDUM FOR DEPUTY COMMISSIONER FOR MODERNIZATION &  
CHIEF INFORMATION OFFICER

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

FROM: Pamela J. Gardiner  
Acting Inspector General

SUBJECT: Final Audit Report – Although Still Behind in Certifying the  
Security of Sensitive Computer Systems, the Internal Revenue  
Service Has Made Significant Progress (Audit # 200120024)

This report presents the results of our review to determine whether the Internal Revenue Service's (IRS) certification and accreditation process is adequate to ensure that sensitive information systems are secure. This review is a follow up to a prior Treasury Inspector General for Tax Administration (TIGTA) audit report.<sup>1</sup>

The certification and accreditation process is perhaps the single most important information systems security process for Federal agencies. If implemented correctly, this process can help ensure that systems have adequate security controls throughout their life spans. The IRS has at least 269 sensitive systems that must be certified.

Functional executives (i.e., heads of office over business units and major IRS programs) must formally accept the risk of implementing a new information system and ensure that it is certified both before implementation and, subsequently, at least every 3 years. The Office of Security Services is responsible for ensuring that security risks have been identified and that adequate controls have been implemented. The certification and accreditation process has been designated a material weakness for Federal Managers' Financial Integrity Act (FMFIA)<sup>2</sup> purposes since 1997.

---

<sup>1</sup> *Certifying the Security of Internal Revenue Service Computer Systems Is Still A Material Weakness* (Reference Number 20020092, dated June 2000).

<sup>2</sup> Federal Managers' Financial Integrity Act of 1982, 31 U.S.C. §§ 1105, 1113, and 3512 (1994 & Supp. IV 1998).

In summary, the IRS has made progress in improving its certification and accreditation process since our last review 2 years ago. The percentage of certified systems has increased from 10 percent in January 2000 to 39 percent in May 2002. We attribute this increase to the continued use of contractor support to complete much of the certification requirements and an effective certification process within the IRS' Certification Program Office. By the end of Fiscal Year 2002, the IRS projects that 44 percent of sensitive systems will be certified and accredited.

The IRS projection still falls short of the Department of the Treasury's goal of having 65 percent of each agency's sensitive systems certified by September 2002. The Certification Program Office has acquired a web-based software tool that is designed to assist the IRS system owners in certifying their sensitive systems. This tool should enhance the IRS' chances of meeting future Department of the Treasury goals.

There are additional barriers that must be overcome, however. A recent inventory identified another 281 computer systems in addition to the 269 sensitive systems that had been previously identified. Owners for the recently identified systems have since been named and will soon be deciding whether the systems contain sensitive information requiring certification. The potential increase in workload could significantly hamper the IRS in finally catching up with the inventory of uncertified systems. Currently, 41 known systems are in the process of being certified. However, 124 of the known systems have not yet been scheduled for certification and none of the 281 newly identified systems have been scheduled. As a result, the security and privacy of taxpayer data on these systems could be at risk.

We recommended that the Deputy Commissioner for Modernization and Chief Information Officer allocate appropriate resources to ensure the certification of these systems in a timely and orderly fashion. Until all systems are certified or scheduled to be certified within a reasonable time frame, sensitive system certification should continue to be considered a material weakness.

Management's Response: The Chief, Security Services, stated that the IRS recognizes the need for an enterprise-wide commitment to ensure it reduces the backlog of uncertified systems. Security Services, Information Technology Services, Agency-Wide Shared Services, Communications and Liaison, and the four business operating divisions will all have to work toward meeting this goal. Affected executives have pledged their support. Security Services will allocate the appropriate resources to ensure it certifies all sensitive systems within the next 2 years.

In addition, the Director, Mission Assurance, will identify and prioritize sensitive systems needing certification for the next 3 years, identify points of contact for those systems, and establish schedules for completing certification of those systems.

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.

**Although Still Behind in Certifying the Security of Sensitive Computer Systems, the Internal Revenue Service Has Made Significant Progress**

---

**Table of Contents**

Background ..... Page 1

Significant Progress Has Been Made in the Certification and Accreditation Program ..... Page 2

Effective Processes Are Available to Assist System Owners on Meeting Certification Requirements..... Page 3

Additional Resources May Be Required to Certify Sensitive Systems..... Page 4

Recommendation 1: ..... Page 5

Appendix I – Detailed Objective, Scope, and Methodology ..... Page 7

Appendix II – Major Contributors to This Report..... Page 8

Appendix III – Report Distribution List ..... Page 9

Appendix IV – Management’s Response to the Draft Report ..... Page 10

## Although Still Behind in Certifying the Security of Sensitive Computer Systems, the Internal Revenue Service Has Made Significant Progress

---

### Background

---

The Office of Management and Budget Circular A-130 and the Department of the Treasury Security Manual TD P 71-10 require that all information systems that process sensitive but unclassified information (e.g., taxpayer data) be certified and accredited for operation. In addition, these information systems are required to be re-certified and re-accredited at least every 3 years or when significant modifications occur. Certification and accreditation are defined as follows.

- 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 (i.e., system owner) that an information system or network is approved to operate with prescribed security safeguards.

Certification and accreditation is perhaps the single most important information systems security process for Federal agencies. The main purpose of system certification and accreditation is to provide documented evidence that the system meets security standards and the system owners accept the security risks related to its operation. Without this process, there is no assurance that the data within the system will be protected against unauthorized disclosure and access (confidentiality) and from unauthorized modification or destruction (integrity). For the Internal Revenue Service (IRS), this assurance is critical since taxpayer data is highly sensitive and personal.

The IRS has incorporated the information from these guidance documents into its Information Technology Security Policy and Guidance manual. The manual clearly states that functional executives (i.e., heads of office over business units and major IRS programs) are responsible for ensuring that the systems are certified and accredited prior to operation. The IRS' Certification Program Office, under the direction of the Chief, Security Services, and Director, Mission Assurance, is responsible for certifying systems and

## Although Still Behind in Certifying the Security of Sensitive Computer Systems, the Internal Revenue Service Has Made Significant Progress

---

for assisting functional executives on the certification and accreditation of their sensitive systems.

We conducted this review as a follow up to a Treasury Inspector General for Tax Administration audit report on the effectiveness of the IRS' certification and accreditation process.<sup>1</sup> This audit was conducted from December 2001 to April 2002, and included visits to the Certification Program Office of the Office of Security Services in New Carrollton, Maryland. We also made telephone contacts to personnel in the office of Strategic Planning and Client Services.

The audit was conducted in accordance with *Government Auditing Standards*. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

---

### Significant Progress Has Been Made in the Certification and Accreditation Program

---

When we reviewed this program 2 years ago, only 10 percent of sensitive systems had been certified. As of May 2002, the percentage of certified systems had increased to 39 percent. Additional systems are in the process of being certified so that, by October 2002, the Certification Program Office projects that 44 percent of its most current inventory of sensitive systems will be certified.

Since our last review, the Certification Program Office continued to employ the assistance of contractors to complete the bulk of the required elements for system certification, including risk assessments and Security Test and Evaluations. The contractors also developed the necessary computer security, configuration management, and continuity of operations plans along with the trusted facilities manuals<sup>2</sup> and Security Features guides.<sup>3</sup>

During 2001, the Certification Program Office purchased a web-based tool that will help automate the certification

---

<sup>1</sup> *Certifying the Security of Internal Revenue Service Computer Systems Is Still a Material Weakness* (Reference Number 20020092, dated June 2000).

<sup>2</sup> Provides guidance to systems administrators on configuring and administering the security features of a system.

<sup>3</sup> Identifies and describes the security features of a system for the system users.

## Although Still Behind in Certifying the Security of Sensitive Computer Systems, the Internal Revenue Service Has Made Significant Progress

---

process for system owners. This tool, tailored for the IRS by the vendor, can guide the system owners through the certification process and significantly reduce the cost associated with document preparation. At the time of this review, the new tool was still being tested, and the Certification Program Office had begun providing training to the systems owners.

The IRS will still not be able to meet the Department of the Treasury's goal of having 65 percent of sensitive systems certified by the end of Fiscal Year 2002. By implementing the new web-based tool and addressing the findings in this report, we are optimistic that the agency can eventually certify all its sensitive systems.

The certification and accreditation process has been designated a material weakness for Federal Managers' Financial Integrity Act (FMFIA)<sup>4</sup> purposes since 1997. Until all systems are certified or scheduled to be certified within a reasonable time frame, sensitive system certification should continue to be considered a material weakness.

---

### Effective Processes Are Available to Assist System Owners on Meeting Certification Requirements

---

A functional executive should be designated as Principal Accrediting Authority (PAA) for each sensitive system and major application. Each PAA is responsible for ensuring that all necessary documentation is prepared for certification.

The Certification Program Office must review the documentation to evaluate technical and non-technical security features, make a technical judgment of the system's compliance with its stated security requirements, assess the risks associated with operating the system, and most importantly, recommend to the PAA whether or not to accredit the system based on the known risks.

The Certification Program Office, with contractor support, followed these procedures and processes to assist functional owners in getting their systems certified. For each of the 15 sensitive systems we reviewed, we found that the

---

<sup>4</sup> Federal Managers' Financial Integrity Act of 1982, 31 U.S.C. §§ 1105, 1113, and 3512 (1994 & Supp. IV 1998).

## Although Still Behind in Certifying the Security of Sensitive Computer Systems, the Internal Revenue Service Has Made Significant Progress

---

---

### Additional Resources May Be Required to Certify Sensitive Systems

---

security plans, risk assessments, and Security Testing and Evaluation clearly documented compliance to IRS security standards.

The certification files also contained the configuration management plans, continuity of operations plans, trusted facilities manuals, and users' guides. We did not evaluate the adequacy of these plans due to time constraints.

The IRS may find it difficult to maintain its current rate of progress in certifying systems. Out of 269 systems the IRS had originally identified, 104 have been certified and an additional 41 were in the process of being certified. While processes to complete certifications are effective, 124 systems have not been scheduled for certification. Further, we were advised that a recent inventory requested by the Deputy Commissioner identified 281 systems not previously included in the Certification Program Office's database.

If a significant number of these systems contain sensitive information, the IRS may have difficulty obtaining sufficient resources to certify them and the 124 known sensitive systems that the IRS had not yet scheduled for certification.

The responsibility for identifying a system and initiating the process for certification and accreditation of sensitive systems falls on the PAA. We contacted the Divisional Information Officers, who are the primary Information Technology Services contacts for the operating division Commissioners, to obtain information on their respective uncertified sensitive systems.

Based on the responses we received, the IRS had not formally assigned PAA responsibility to individuals to promote accountability for sensitive systems and their certification. Since then, owners of the systems have been named and will soon be deciding whether the systems contain sensitive information requiring certification.

To a large extent, the identification of the PAAs has degraded during the past few years while the IRS has undertaken a massive reorganization in response to the IRS

## Although Still Behind in Certifying the Security of Sensitive Computer Systems, the Internal Revenue Service Has Made Significant Progress

---

Restructuring and Reform Act of 1998.<sup>5</sup> Executive owners of sensitive systems cannot be easily defined by their current organizational responsibilities. For example, sensitive systems that were used and owned by the former Examination organization can now be used by the Wage and Investment Division and the Small Business/Self-Employed Division. Since no clear functional delineation is apparent, the assignment of the PAA was uncertain.

The Certification Program Office relied on functional executives to keep them apprised of current systems. Because the Certification Program Office was not required to follow-up with systems owners or did not know who the PAA was, its database had not been updated for several years.

### Recommendation

1. Once all sensitive systems have been identified, the Deputy Commissioner for Modernization and Chief Information Officer should ensure they are prioritized and allocate appropriate resources to ensure that all sensitive systems are certified within a reasonable time frame.

Management's Response: The Chief, Security Services, stated that the IRS recognizes the need for an enterprise-wide commitment to ensure it reduces the backlog of uncertified systems. Security Services, Information Technology Services, Agency-Wide Shared Services, Communications and Liaison, and the four business operating divisions will all have to work toward meeting this goal. Affected executives have pledged their support. Security Services will allocate the appropriate resources to ensure it certifies all sensitive systems within the next 2 years.

---

<sup>5</sup> IRS Restructuring and Reform Act of 1998, Pub. L. No. 105-206, 112 Stat. 685 (codified as amended in scattered sections of 2 U.S.C., 5 U.S.C., 5 U.S.C. app., 16 U.S.C., 19 U.S.C., 22 U.S.C., 23 U.S.C., 26 U.S.C., 31 U.S.C., 38 U.S.C., and 49 U.S.C.).

## **Although Still Behind in Certifying the Security of Sensitive Computer Systems, the Internal Revenue Service Has Made Significant Progress**

---

In addition, the Director, Mission Assurance, will identify and prioritize systems needing security certification for the next 3 years, define the results indicator as the percentage of systems certified in a fiscal year, and identify business owner and Information Technology Service contact points responsible for ensuring sensitive systems are certified.

**Detailed Objective, Scope, and Methodology**

The overall audit objective was to determine if the Internal Revenue Service (IRS) adequately addressed security of its information systems through the certification and accreditation process. This review is a follow up to an earlier audit by The Treasury Inspector General for Tax Administration (TIGTA) entitled *Certifying the Security of Internal Revenue Service Computer Systems Is Still a Material Weakness* (Reference Number 200020092, dated June 2000). To accomplish our objective, we performed the following audit steps.

- I. Determined if the IRS took corrective actions, as stated in its response to the prior TIGTA audit report on the IRS certification and accreditation program, to certify all systems prior to operation and assure Interim Authorities to Operate are timely converted to unconditional certifications. Determined if system owners are adequately trained on the certification process and kept apprised of certification requirements. Also, determined if IRS adequately budgets funds for the certification process.
- II. Randomly selected a judgmental sample of 15 of the 104 certified systems to determine if the associated Certification Packages included all the required documentation (a random sample was used because we were not planning on projecting the results). Determined the current certification status of all IRS sensitive systems. Contacted representatives from the Certification Program Office and the Office of Strategic Planning and Client Services to validate information on sensitive systems.
- III. Determined if current government directives and laws provide opportunities to improve the efficiency of the certification and accreditation process. Also, randomly selected a judgmental sample of 15 certified systems to determine if certification risk assessments and security plans were used as the primary guidance for Security Testing and Evaluation. Determined if the IRS must account to other government agencies on its systems certification status.

**Major Contributors to This Report**

Scott E. Wilson, Assistant Inspector General for Audit (Information Systems Programs)  
Steve Mullins, Director  
Kent Sagara, Audit Manager  
Dan Ardeleano, Senior Auditor  
William Lessa, Senior Auditor  
Larry Reimer, Senior Auditor

**Although Still Behind in Certifying the Security of Sensitive Computer Systems, the Internal Revenue Service Has Made Significant Progress**

---

**Appendix III**

**Report Distribution List**

Commissioner N:C  
Deputy Commissioner N:DC  
Chief, Security Services M:S  
Director, Strategic Planning & Client Services M:SP  
Director, Mission Assurance M:S:A  
Chief, Certification Program Office M:S:A:C  
Chief Counsel CC  
National Taxpayer Advocate TA  
Director, Legislative Affairs CL:LA  
Director, Office of Program Evaluation and Risk Analysis N:ADC:R:O  
Office of Management Controls N:CFO:F:M  
Audit Liaisons:  
    Deputy Commissioner for Modernization & Chief Information Officer M:SP:P:O  
    Security Services M:S

**Although Still Behind in Certifying the Security of Sensitive Computer Systems, the Internal Revenue Service Has Made Significant Progress**

---

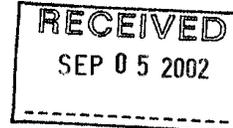
Appendix IV

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



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

SEP - 5 2002



MEMORANDUM FOR TREASURY INSPECTOR GENERAL FOR TAX  
ADMINISTRATION

FROM: Len Baptiste *Len Baptiste*  
Chief, Security Services

SUBJECT: Response to Draft Audit Report – Although Still Behind in  
Certifying the Security of Sensitive Computer Systems, the IRS  
Has Made Significant Progress (Audit # 200120024)

Our management goal is to achieve an enhanced security program that effectively manages risks. In this regard, we have actively addressed our certification and accreditation problem by:

- Establishing an approach to more efficiently and effectively certify information systems
- Developing a repeatable process for the system security certification and accreditation (C&A) process
- Developing a repeatable process for conducting Security Tests and Evaluations.
- Procuring an automated Web tool for C&A
- Developing a central repository for certification data
- Providing training to end-users on the C&A process and the Web C&A Tool

In addition, we continue to assist project owners in the certification process.

The improved C&A process reduces the paperwork burden and the certification backlog of systems. The percentage of certified systems has increased from 10 percent in January 2000 to 39 percent in May 2002. We are certifying all new systems before deployment while we continue to work the backlog of uncertified systems in a timely manner.

The IRS recognizes we need an enterprise-wide commitment to ensure we reduce the backlog of uncertified systems. Security Services, Information Technology Services, Agency-Wide Shared Services, Communications and Liaison, and our four business operating divisions will all have to work toward meeting this goal. Affected executives have pledged their support. We will allocate the appropriate resources to ensure we certify all sensitive systems within the next two years.

**Although Still Behind in Certifying the Security of Sensitive Computer Systems, the Internal Revenue Service Has Made Significant Progress**

---

2

If you have any questions, please call me at (202) 622-8910, or Colleen Murphy, Director, Mission Assurance at (202) 283-4351.

Attachment

## **Although Still Behind in Certifying the Security of Sensitive Computer Systems, the Internal Revenue Service Has Made Significant Progress**

---

Response to Draft Audit Report – Although Still Behind in Certifying the Security of Sensitive Computer Systems, the IRS Has Made Significant Progress (Audit # 200120024)

### **RECOMMENDATION #1**

Once all sensitive systems have been identified, the Deputy Commissioner for Modernization and Chief Information Officer should ensure they are prioritized and allocate appropriate resources to ensure that all sensitive systems are certified within a reasonable time frame.

### **ASSESSMENT OF CAUSE**

Our systems lacked certification and accreditation; all sensitive systems were not properly identified; and technical difficulties (i.e. communications infrastructure) may have hindered compliance.

### **CORRECTIVE ACTION #1**

We will:

- Identify and prioritize systems needing security certification for the next three years
- Define Results Indicator -- The percentage of systems certified in a fiscal year
- Identify points of contact from both business owners and Information Technology Services, responsible for ensuring sensitive systems are certified
- Complete schedule to certify systems with results indicators

### **IMPLEMENTATION DATE OF CORRECTIVE ACTION**

**Completed:**

**Proposed:** October 1, 2004

### **RESPONSIBLE OFFICIAL**

Director, Mission Assurance M:S:A