# The Certification and Accreditation of Computer Systems Should Remain in the Computer Security Material Weakness

August 2004

Reference Number:  2004-20-129

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

August 9, 2004

MEMORANDUM FOR CHIEF, MISSION ASSURANCE

Gordon C. Milbourn III

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

SUBJECT: Final Audit Report – The Certification and Accreditation of Computer Systems Should Remain in the Computer Security Material Weakness (Audit # 200420005)

This report presents the results of our review of the effectiveness of Internal Revenue Service (IRS) actions to resolve the certification and accreditation vulnerabilities associated with the computer security material weakness. The Department of the Treasury requested that the Treasury Inspector General for Tax Administration (TIGTA) provide an independent assessment of the effectiveness of the IRS' actions to address the material weakness. This report is from one of five reviews conducted during this fiscal year to meet this request.

In summary, the IRS has made commendable progress in certifying its many computer systems, but additional work remains to be performed before this area within the computer security material weakness can be downgraded. The IRS Office of Mission Assurance has initiated efforts to revamp the certification process by placing all IRS systems into one of four categories. As of February 2004, these categories were General Support Systems (29 systems), Major Applications (27 systems), Applications of Interest (31 systems), and Other Applications (312 systems).

The Chief, Mission Assurance, established certification requirements for the General Support Systems, Major Applications, and Applications of Interest. Other Applications will be mapped to the appropriate General Support System, and less stringent security self-assessments will be used as a basis to review security in the Other Applications. As of May 2004, 36 (12 percent) of the 312 Other Applications had not yet been mapped.

We concur with the overall approach for classifying systems in the new categories based on risks and for developing customized certification requirements for each of the categories. The IRS is following guidance from the Federal Information Security Management Act[1] and the National Institute of Standards and Technology (NIST).[2]

However, the IRS has not certified and accredited enough systems to downgrade this area within the computer security material weakness. As of February 2004, the IRS reported that 58 (67 percent) of the 87 General Support Systems, Major Applications, and Applications of Interest had been certified. In addition, only 18 (31 percent) of the 58 certified systems had been accredited. The unaccredited systems are in use by the IRS, although no IRS manager has accepted responsibility for the respective systems' security. In the past, the IRS has not monitored the accreditation process to ensure accreditations were completed and accountability over the systems was maintained. The Office of Mission Assurance has initiated efforts to begin tracking accreditations of systems and when it expects accreditations to be completed, although no formal process to do this has been established.

We recommended the Chief, Mission Assurance, keep the certification and accreditation of computer systems as part of the computer security material weakness until a sufficient number of systems has been certified. We suggested the IRS follow the lead provided by the President's Management Agenda (PMA),[3] which states that at least 90 percent of the systems should be certified and accredited for agencies to get a "green" status. In addition, the Chief, Mission Assurance, should continue mapping Other Applications to General Support Systems to ensure all Other Applications are included in a General Support Systems certification and accreditation, and should establish a formal process to monitor accreditations and report noncompliance, as needed, to the Deputy Commissioners to ensure accreditations are completed.

Management's Response: The Chief, Mission Assurance, disagreed with the recommendation that certification and accreditation remain as part of the computer security material weakness. He contended the IRS has exceeded the goal it set in 2002, to certify and accredit 75 percent of IRS systems known at that time. The Chief, Mission Assurance, agreed with the other two recommendations. He has developed a plan to ensure all Other Applications are correctly mapped to General Support Systems and has implemented a process to require accreditation memoranda be returned to his office. This will allow him to ensure accreditations have been completed and to monitor and report any noncompliance to the IRS Deputy Commissioners on a yearly basis. Management's complete response to the draft report is included as Appendix V.

Office of Audit Comment: We strongly believe the certification and accreditation of sensitive systems should remain as part of the computer security material weakness.

[1] Pub. L. No. 107-347, Title III, 116 Stat. 2946 (2002).

[2] The NIST, under the Department of Commerce, is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all Federal Government agency operations and assets.

[3] The PMA outlines the President's strategy for improving the management and performance of the Federal Government. Congressional testimony from the Honorable Karen Evans from the OMB on March 16, 2004, referred to the President's Management Agenda as an important mechanism for acknowledging agency Information Technology security progress and highlighting significant problems.

Since 2002, when the IRS established its baseline goal for closing the certification and accreditation material weakness area, there have been two significant developments that lead us to conclude this issue has not yet been resolved.

First, agencies' certification and accreditation performance has received increased attention and oversight by the Office of Management and Budget (OMB). The Expanding E-Government Scorecard under the PMA has established that 90 percent of systems should be certified and accredited for an agency to receive "green" status in this area and that 80 percent compliance receive "yellow" status. Therefore, we believe a 75 percent performance measure, while acceptable in 2002, is not in line with the current Government-wide goals.

Second, the IRS' systems inventory count in 2002, which served as the baseline for the 75 percent goal, has proven to be inaccurate. Since that time, IRS management has rigorously worked to establish an accurate inventory of systems. As a result, both the number of systems and the number requiring certification and accreditation have been revised. Based on this more accurate data, and as stated in this report, the IRS had certified 67 percent of its major systems, as of February 2004.

In its response, the IRS proposed to close certification and accreditation as a material weakness area and then assess the prudence of reopening it as a new material weakness. The benefit of this approach is not clear. In our opinion, the weakness has existed for years and has not yet been corrected to meet the goals of the PMA. Accordingly, we believe it should remain as part of the computer security material weakness and we intend to elevate our disagreement to the Department of the Treasury for resolution.

The Deputy Commissioner for Operations Support is responsible for ensuring the IRS Commissioner submits a written reply to the Assistant Secretary for Management and Chief Financial Officer of the Department of the Treasury within 30 calendar days of the final report issuance date. This reply should explain the IRS' reasons for the lack of agreement with the recommendation contained in this audit report. The IRS Commissioner will provide a copy of the reply to the TIGTA. Resolution shall be made within a maximum of 6 months after issuance of a final TIGTA audit report, in accordance with OMB Circular A-50.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions or Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

# Table of Contents

# The Certification and Accreditation of Computer Systems Should Remain in the Computer Security Material Weakness

## Background

The Federal Managers' Financial Integrity Act[1] requires that each agency conduct annual evaluations of its systems of internal accounting and administrative control and submit an annual statement on the status of the agency's system of management controls. As part of the evaluations, agency managers identify control areas that can be considered material or significant weaknesses.

The Department of the Treasury has defined a material weakness as, "shortcomings in operations or systems which, among other things, severely impair or threaten the organization's ability to accomplish its mission or to prepare timely, accurate financial statements or reports." The Office of Management and Budget (OMB) monitors' progress on these weaknesses.

The Department of the Treasury also defines weaknesses of lesser importance, sometimes referred to as Reportable Conditions or Significant Control Deficiencies. These are problematic issues which do not rise to the level of materiality but which warrant special management attention to ensure improvement rather than deterioration to the point at which they become material weaknesses. The OMB does not monitor progress on these weaknesses.

In 1995, the Internal Revenue Service (IRS) began monitoring the certification and accreditation process of its sensitive computer systems as a potential management control weakness. In 1997, the IRS officially reported it as a material weakness.

Certification and accreditation, as defined and required by the OMB for all Federal Government automated information systems,[2] is a process to provide assurance that adequate security controls are in place over computer systems. Systems should be certified and accredited before being implemented and at least every 3 years thereafter or when a significant change is made that affects the system, whichever occurs first.

Certification is the comprehensive evaluation of the technical and non-technical security controls and the

[1] 31 U.S.C.: §§ 1105, 1113, and 3512 (2000).

[2] OMB Circular A-130, *Management of Federal Information Resources,* dated February 1996.

identification of any weaknesses with those controls or lack thereof. Accreditation is an authorization granted by a management official to operate the system based on the evaluation of the security controls. It is a statement that the management official (i.e., the accrediting official) is aware of, understands, and accepts responsibility for the risks associated with placing the system into operation. A summary of the certification and accreditation process is provided in Appendix IV.

In October 2002, the IRS consolidated all computer security-related material weaknesses, including the certification and accreditation of sensitive systems, into one material weakness.[3] The Department of the Treasury requested that the Treasury Inspector General for Tax Administration provide an independent assessment of the effectiveness of the IRS' actions to address the overall computer security material weakness. This review is one of five reviews conducted during this fiscal year to meet this request.

This review was conducted in the Office of Mission Assurance facilities at the IRS Headquarters in New Carrollton, Maryland, during the period August 2003 through April 2004. 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.

## More Actions Need to Be Completed Before the Certification and Accreditation Material Weakness Area Is Downgraded

The IRS has made commendable progress in certifying its many computer systems, but additional work remains to be performed before this area within the computer security material weakness can be downgraded. Determining the number of systems to be certified and accredited has been a

[3] The computer security material weakness consists of nine areas: (1) Network Access Controls; (2) Key Computer Applications and System Access Controls; (3) Configuration of Software; (4) Functional Business, Operating, and Program Units' Security Roles and Responsibilities; (5) Segregation of Duties Between System and Security Administrators; (6) Contingency Planning and Disaster Recovery; (7) Monitoring of Key Networks and Systems; (8) Security Training; and (9) Certification and Accreditation.

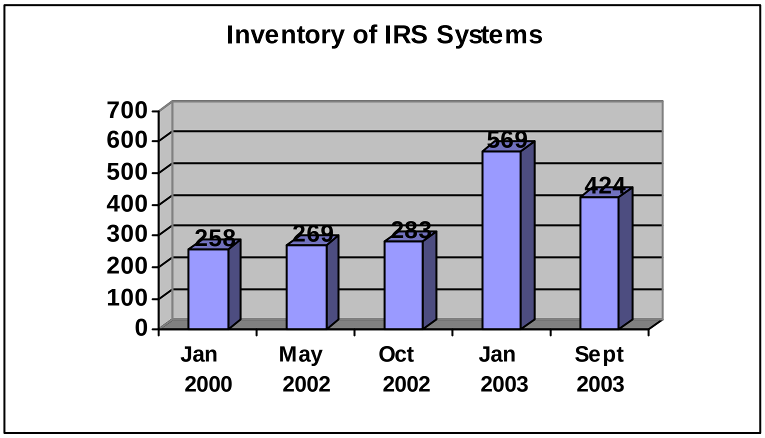
challenge. In addition, a sufficient number of systems has not been certified and accredited.

**Determining the number of systems to be certified and accredited has been a challenge**

When we conducted an audit in this area in January 1999, the IRS had certified 10 percent of its sensitive systems.[4] In May 2002, the certification percentage had increased to 39 percent, based on a follow-up review we performed.[5] The IRS established a certification goal of 75 percent by September 2003 to close this material weakness and reported to the Department of the Treasury that it had met this goal.

However, the percentage of systems certified has always been questionable because the IRS has had difficulty determining the number of systems to be certified. In January 2000, the IRS reported it had 258 computer systems and it has since reported a different number every year, as reflected in Chart 1.

**Chart 1**



*Source: The IRS Office of Mission Assurance.*

This system inventory fluctuation was a result of the IRS' own changing interpretation of what it considered a system.

[4] *Certifying the Security of Internal Revenue Service Computer Systems Is Still A Material Weakness* (Reference Number 2000-20-092, dated June 2000).
[5] *Although Still Behind in Certifying the Security of Sensitive Computer Systems, the Internal Revenue Service Has Made Significant Progress* (Reference Number 2002-20-165, dated September 2002).

At its peak in January 2003, the IRS system count consisted of any computer program that resembled a system. For example, the inventory included those programs that were not even information systems, such as spreadsheets and other personal productivity tools. After a concerted effort to purify its system inventory number, the IRS reported it had 424 sensitive systems, as of September 2003.

When the IRS reported it had met the 75 percent certification goal of its sensitive systems, it had based its accomplishments on the number of sensitive systems known in October 2002, which totaled 283. The October 2002 date represented when the IRS and the Department of the Treasury agreed to the 75 percent milestone. Thus, the IRS reported that it had certified 232 (82 percent) of 283 systems.

We believe meeting the 75 percent milestone on an outdated number of systems does not warrant the downgrading or closing of the certification and accreditation material weakness area. The IRS operated an additional 141 systems that were not considered when the IRS calculated its accomplishments. Therefore, we concluded that, as of September 2003, the IRS had certified 232 (55 percent) of 424 systems.

The Department of the Treasury recognized the differences in these accomplishments. In December 2003, it gave the IRS 60 days to straighten out the count of its sensitive systems for certification and accreditation purposes. To meet this mandate as well as to address the certification and accreditation material weakness area, the IRS planned to take the following actions:

- Establish new system categories based on risk level and mission criticality, ensuring methodology and deliverables are consistent with guidance from the Federal Information Security Management Act

(FISMA)[6] and the National Institute of Standards and Technology (NIST).[7]

- Establish certification and accreditation requirements for each of the new system categories.
- Certify and accredit systems necessary to downgrade or close the material weakness area.

To establish new system categories, the Office of Mission Assurance reevaluated the IRS' systems inventory to definitively identify the total number of systems and developed a new systems categorization methodology. While conducting this effort, the Office of Mission Assurance found that some systems were no longer operational and others could be considered as a subsystem of another system.

In February 2004, the Office of Mission Assurance presented its new methodology, which placed 399 systems into 1 of 4 categories based on risk, defined as follows:

General Support Systems (29 systems) provide necessary Information Technology infrastructure support to applications and business functionality. Compromise of these systems would have a severe adverse effect on the IRS mission, tax administration functions, and/or employee welfare. Subcategories consist of telecommunications, modernization, computing platforms, and other networks.

Major Applications (27 systems) require special attention to security because of the severe adverse effect that compromise of these applications would have on the IRS mission, tax administration functions, and/or employee welfare. This category includes production modernization systems, consolidated applications on the same platform, and financial systems based on size and scope.

[6] Pub. L. No. 107-347, Title III, 116 Stat. 2946 (2002).

[7] The NIST, under the Department of Commerce, is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all Federal Government agency operations and assets. NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, provides guidelines for executive agencies to help achieve more secure information systems within the Federal Government.

Applications of Interest (31 systems) do not possess the level of interest and size or scope of the Major Application category but require additional levels of control because, based on business functionality, level of exposure, or third party interest, compromise would significantly degrade the IRS' mission and tax administration operation.

Other Applications (312 systems) do not generally require additional security safeguards above those provided by the General Support System.

In establishing certification and accreditation requirements, the Office of Mission Assurance has proposed procedures that would assign varying levels of certification requirements to the four categories.  The procedures require that General Support Systems and Major Applications receive a full independent certification as well as accreditation.  The procedures specify that Applications of Interest receive various levels of certification depending on the results of a risk analysis.

The IRS did not plan to conduct separate testing on the Other Applications.  Instead, it planned to map the Other Applications to a General Support System and rely primarily on the security controls existing in the underlying network of the General Support System, which will be required to be certified and accredited.  As of May 2004, the IRS had not yet mapped 36 (12 percent) of the 312 systems in the Other Applications category to a General Support System.

We also raised concerns with this approach due to the sensitivity of data on some of the Other Applications and the need to maintain security controls on the applications as well as the General Support System.

The Office of Mission Assurance plans to continue discussions with IRS personnel and to conduct site visitations to complete this mapping effort, as well as to ensure all systems in the Other Applications category are accurately categorized.

In May 2004, the Chief, Mission Assurance, decided that security self-assessments, as required by the FISMA, would be conducted for the Other Applications.  These self-assessments, which are less stringent than the certification requirements for the other three categories, will provide some review of security controls on the Other Applications.

We concur with the overall approach the IRS is now taking with the categorization of its systems and its new certification requirements. This approach will allow the IRS to focus most of its certification efforts on the General Support Systems, Major Applications, and Applications of Interest, while still providing some assessment of controls on the Other Applications. The approach is substantially consistent with NIST guidance.

### A sufficient number of systems has not been certified and accredited

The IRS has not certified enough systems to downgrade this material weakness. As of February 2004, the IRS reported it had certified 58 (67 percent) of the 87 General Support Systems, Major Applications, and Applications of Interest.

Once systems have been certified, the Office of Mission Assurance provides various documents to the accrediting officials for consideration. These documents include current system security plans, security assessment reports, and actions needed to correct deficiencies noted during testing.

After reviewing certification information, accrediting officials have three choices. They can:

- Submit full authorization to operate as is.
- Provide an interim approval to operate pending the correction of vulnerabilities.
- Deny authorization to operate.

We found that accrediting officials were not complying with the accreditation procedures. Only 18 (31 percent) of the 58 certified systems had been accredited. The unaccredited systems are already in use by the IRS. However, no IRS employee is accountable for the security of those systems that have not been accredited. Consequently, unaccredited systems are more likely to become operational with known security vulnerabilities, thus placing the systems and their data at risk.

Business unit system owners are primarily responsible for accrediting their systems. In the past, the IRS has not monitored the accreditation process to ensure accreditations were completed and accountability over the systems was maintained. While it has no authority over the accreditation process, the Office of Mission Assurance has initiated efforts to begin tracking accreditations of systems and when it expects accreditations to be completed, although no formal process to do this has been established.

Without an effective certification and accreditation process, the IRS cannot make informed decisions on the risks associated with its systems. Until the process provides a more thorough assessment of risk for systems and applications, we believe the additional oversight provided by externally reporting this weakness area is appropriate.

## Recommendations

The Chief, Mission Assurance, should:

1. Keep the certification and accreditation of computer systems as part of the computer security material weakness until a sufficient number of systems has been certified and accredited. We suggest the IRS follow the Expanding E-Government Scorecard for Information Technology Security under the President's Management Agenda (PMA),[8] which states that at least 90 percent of the systems should be certified and accredited for agencies to receive "green" status in this area.

Management's Response: The Chief, Mission Assurance, disagreed with this recommendation and contended the IRS has exceeded the goal it set in 2002, to certify and accredit 75 percent of IRS systems.

Office of Audit Comment: We strongly believe that certification and accreditation of sensitive systems should

[8] The PMA outlines the President's strategy for improving the management and performance of the Federal Government. Congressional testimony from the Honorable Karen Evans from the OMB on March 16, 2004, referred to the President's Management Agenda as an important mechanism for acknowledging agency Information Technology security progress and highlighting significant problems.

remain part of the computer security material weakness. Since 2002, when the IRS established its baseline goal for closing the certification and accreditation material weakness area, there have been two significant developments that lead us to conclude this issue has not yet been resolved.

First, agencies' certification and accreditation performance has received increased attention and oversight by the OMB. The Expanding E-Government Scorecard under the PMA has established that 90 percent of systems should be certified and accredited for an agency to receive "green" status in this area and that 80 percent compliance receive "yellow" status. Therefore, we believe a 75 percent performance measure, while acceptable in 2002, is not in line with the current Government-wide goals.

Second, the IRS' systems inventory number in 2002, which served as the baseline for the 75 percent goal, has proven to be inaccurate. Since that time, IRS management has rigorously worked to establish an accurate inventory of systems. As a result, both the number of systems and the number requiring certification and accreditation have been revised. Based on this more accurate data, and as stated in this report, the IRS had certified 67 percent of its major systems, as of February 2004.

In its response, the IRS proposed to close certification and accreditation as a material weakness area and then assess the prudence of reopening it as a new material weakness. The benefit of this approach is not clear. In our opinion, the weakness has existed for years and has not yet been corrected to meet the goals of the PMA. Accordingly, we believe it should remain as part of the computer security material weakness.

2. Complete the mapping of systems in the Other Applications category to the General Support Systems to ensure all Other Applications are included in a General Support Systems certification and accreditation. Site visitations should be completed as planned to ensure all systems, including Other Applications, have been appropriately categorized and receive the necessary certification attention.

Management's Response: The Chief, Mission Assurance, agreed with this recommendation and the IRS has developed a plan to ensure all Other Applications are correctly mapped to General Support Systems as part of its new certification and accreditation approach.

3. Establish a formal process to monitor accreditations and report noncompliance, as needed, to the Deputy Commissioners to ensure accreditations are completed.

Management's Response: The Chief, Mission Assurance, agreed with this recommendation and has implemented a process that requires all accreditation memoranda to be returned to his office and provides the IRS Deputy Commissioners with a report of systems not accredited on an annual basis.

## Appendix I

### Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether the Internal Revenue Service (IRS) has effectively resolved vulnerabilities associated with its computer security material weakness. The IRS has segregated this material weakness into nine areas, one of which covers the certification and accreditation of computer systems. To accomplish our objective, we:

I. Determined if the applications in the revised master inventory have been appropriately categorized.

   A. Evaluated the criteria used for categorizing systems and applications into the four categories (General Support Systems, Major Applications, Applications of Interest, and Other Applications).

   B. If any systems were miscategorized, determined the reasons why.

II. Determined if certification requirements established for each of the four categories were appropriate.

   A. Identified the specific certification requirements for each of the four categories.

   B. Evaluated the certification requirements for each category to determine whether adequate security was reflected for each category. If any categories had insufficient certification requirements, we determined the reason why.

III. Determined how the revised certification and accreditation approach and system inventory count affected the material weakness definition and assessed the current status of the material weakness.

IV. Assessed the certification and accreditation process in terms of the general coverage of certification testing, the identification of security vulnerabilities, and the compliance with accreditation requirements.

V. Determined how many systems had been certified and accredited. For systems not certified or accredited, we held discussions with Office of Mission Assurance staff to determine the reasons why.

## Appendix II

### Major Contributors to This Report

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)
Steve Mullins, Director
Kent Sagara, Audit Manager
Mary Jankowski, Senior Auditor
Thomas Nacinovich, Senior Auditor
Joan Raniolo, Senior Auditor
Charles Ekholm, Auditor

## Appendix III

## Report Distribution List

Commissioner  C
Office of the Commissioner – Attn:  Chief of Staff  C
Deputy Commissioner for Operations Support  OS
Chief Information Officer  OS:CIO
Director, Certification Testing, Evaluation and Assessment  OS:MA:CT
Director, Modernization and Systems Security Engineering  OS:MA:M
Director, Portfolio Management  OS:CIO:R:PM
Chief Counsel  CC
National Taxpayer Advocate  TA
Director, Office of Legislative Affairs  CL:LA
Director, Office of Program Evaluation and Risk Analysis  RAS:O
Office of Management Controls  OS:CFO:AR:M
Audit Liaisons:
    Chief Information Officer  OS:CIO
    Chief, Mission Assurance  OS:MA

## Appendix IV

### Summary of the Certification and Accreditation Process

The following description is derived from the *Guide for the Security Certification and Accreditation of Federal Information Systems*, National Institute of Standards and Technology (NIST) Special Publication 800-37 (dated May 2004).[1] It is a brief summary of steps an agency should take in completing a certification and accreditation.

The evaluation of security controls to enable a decision on whether to place a computer system into operation is known as certification. Steps to certify a computer system include:

1. Review the system security plan and confirm that the contents of the plan are consistent with an initial assessment of risk.
2. Notify concerned agency officials as to the need for security certification and accreditation; determine the resources needed to carry out the effort; and prepare a plan to execute the security certification and accreditation activities, including a proposed schedule and key milestones.
3. Independently analyze security categorizations, obtain an independent analysis of the system security plan, update as needed based on the results of the independent analysis, and obtain acceptance of the system security plan by the authorizing official and senior agency information security officer.[2]
4. Gather supporting information needed for the assessment (system requirements and design documents, security control implementation evidence, etc.). Evaluate the security controls and document results of the evaluation in a security assessment report.
5. Provide the certification agent with the security assessment report, update the system security plan as needed, assemble the final security accreditation package, and submit it to the authorizing official.

The senior agency official's authorization to place a computer system into operation based on the certification evaluation is known as accreditation. Steps to accredit a computer system include:

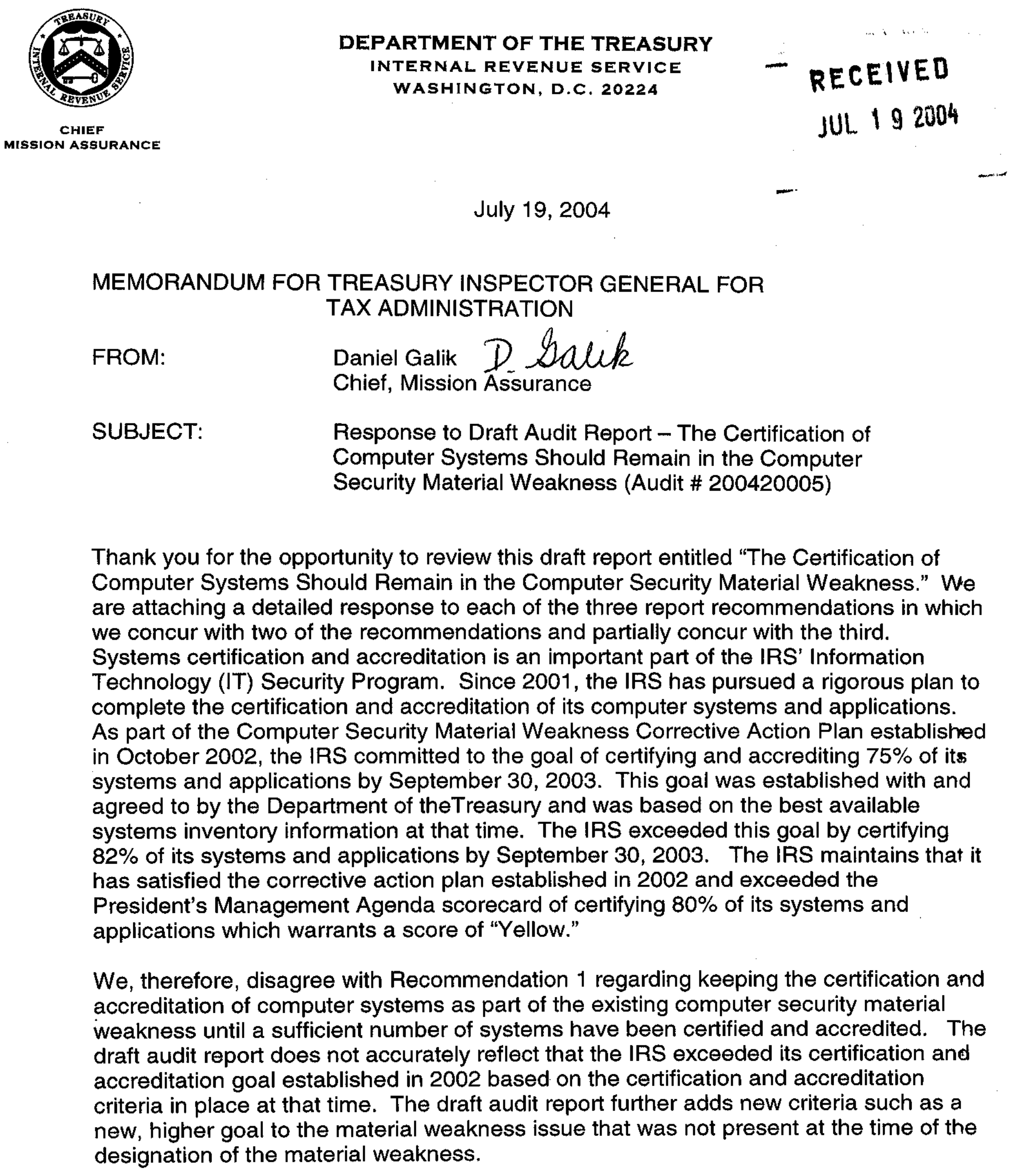
[1] The NIST, under the Department of Commerce, is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all Federal Government agency operations and assets. NIST Special Publication 800-37 provides guidelines for executive agencies to help achieve more secure information systems within the Federal Government.

[2] NIST supplemental guidance states that a non-independent self-assessment may be used for low-impact systems. Additional guidance relating to low-impact systems is also provided on other steps in the certification and accreditation process, generally allowing for a streamlined process and indicating that independence is not required.

1. Determine residual risk to operations or assets based on vulnerabilities and any planned or completed corrective actions to reduce vulnerabilities, determine if the actual residual risk is acceptable, and prepare the final security accreditation decision letter.
2. Transmit the final security accreditation package to the appropriate individuals and organizations and update the system security plan with the latest information from the accreditation decision.

## Appendix V

## Management's Response to the Draft Report



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

CHIEF
MISSION ASSURANCE

July 19, 2004

MEMORANDUM FOR TREASURY INSPECTOR GENERAL FOR
TAX ADMINISTRATION

FROM: Daniel Galik D Galik
Chief, Mission Assurance

SUBJECT: Response to Draft Audit Report – The Certification of Computer Systems Should Remain in the Computer Security Material Weakness (Audit # 200420005)

Thank you for the opportunity to review this draft report entitled "The Certification of Computer Systems Should Remain in the Computer Security Material Weakness." We are attaching a detailed response to each of the three report recommendations in which we concur with two of the recommendations and partially concur with the third. Systems certification and accreditation is an important part of the IRS' Information Technology (IT) Security Program. Since 2001, the IRS has pursued a rigorous plan to complete the certification and accreditation of its computer systems and applications. As part of the Computer Security Material Weakness Corrective Action Plan established in October 2002, the IRS committed to the goal of certifying and accrediting 75% of its systems and applications by September 30, 2003. This goal was established with and agreed to by the Department of theTreasury and was based on the best available systems inventory information at that time. The IRS exceeded this goal by certifying 82% of its systems and applications by September 30, 2003. The IRS maintains that it has satisfied the corrective action plan established in 2002 and exceeded the President's Management Agenda scorecard of certifying 80% of its systems and applications which warrants a score of "Yellow."

We, therefore, disagree with Recommendation 1 regarding keeping the certification and accreditation of computer systems as part of the existing computer security material weakness until a sufficient number of systems have been certified and accredited. The draft audit report does not accurately reflect that the IRS exceeded its certification and accreditation goal established in 2002 based on the certification and accreditation criteria in place at that time. The draft audit report further adds new criteria such as a new, higher goal to the material weakness issue that was not present at the time of the designation of the material weakness.

While the draft audit report does reflect the IRS' efforts to revise its systems inventory to bring the IRS' overall certification accreditation process in line with the Office of Management and Budget (OMB) and National Institute of Standards and Technology (NIST) guidance, the draft audit report does not assess whether the new accreditation processes warrant a new designation of material weakness. The IRS does not believe that it is cost effective or prudent to keep the original material weakness open or modify the original basis upon which the material weakness was designated because those conditions no longer exist.

In February 2004, the IRS conducted an evaluation of its overall approach to information systems categorization and security certification and accreditation. As a result of the evaluation, the IRS developed a comprehensive information security program strategy that will validate the IRS inventory of systems and provide a new practical and cost effective certification and accreditation approach that will be fully compliant with the Federal Information Security Management Act (FISMA), OMB, and NIST guidance. The IRS' strategy is consistent with FISMA, which requires the agency to utilize a risk management approach that properly balances business requirements and risks in providing appropriate information security protections and utilizing cost effective security processes. The IRS' revised strategy and supporting details related to the total number of systems and applications to be certified and accredited were reported to Department of the Treasury and forwarded to OMB in February 2004. Both the Department of theTreasury and OMB have endorsed the IRS' efforts to more accurately report its systems inventory and the IRS' new certification and accreditation approach. The IRS is vigorously implementing this strategy which will result in all applicable systems and applications being fully certified and accredited in early to mid-2005.

However, because the IRS believes it is critical to fully certify and accredit its revised systems inventory to ensure that its systems and data are appropriately safeguarded we will assess whether it is prudent to designate the new approach as a new material weakness.

We agree with recommendations two and three regarding the complete mapping of "Other Applications to General Support Systems" and establishing a formal process to monitor and report on accreditation status, respectively. The IRS' new cost effective certification and accreditation approach will ensure that all "Other Applications" are properly mapped to General Support Systems and we will report the status of all system accreditations as part of our 2004 FISMA review process.

If you have any questions, please contact me at (202) 622-8910 or Rose Hernandez, Director, Certification, Testing, Evaluation, and Assessment, at (202) 283-4500.

Attachment

**Management Response to Draft Audit Report –The Certification and Accreditation of Computer Systems Should Remain in the Computer Security Material Weakness (Audit # 200420005)**

**RECOMMENDATION # 1:** The Chief, Mission Assurance, should keep the certification and accreditation of computer systems as part of the computer security material weakness until a sufficient number of systems have been certified and accredited. We suggest the IRS follow the Expanding E-Government Scorecard for Information Technology Security under the President's Management Agenda, which states that at least 90 percent of the systems should be certified and accredited for agencies to receive "green" status in this area.

**CORRECTIVE ACTION TO RECOMMENDATION #1:**

a) Mission Assurance partially concurs with this recommendation. The draft audit report places the gross number of systems that have been certified and accredited as the sole determiner of material weakness. The draft audit report does not factor in the strength of the processes used to complete security certifications or the viability of the IRS' new certification and accreditation approach. The draft audit report further cites the fluctuation of the IRS' systems inventory as a supporting reason for not closing the material weakness. However, the report notes that many of the systems previously counted or identified as systems were "any computer program that resembled a system" including programs that were not even information systems, such as spreadsheets and other personal productivity tools and should not have been expected to be certified and accredited. The report also does not reflect that systems inventories will naturally fluctuate as a matter of doing business. For example, systems will be retired or merged with other systems and new systems will be developed resulting in the gross number of systems being changed. The IRS agrees that its systems inventory was in sore need of being scrubbed and brought into line with applicable Office of Management and Budget (OMB) and National Institute of Standards and Technology (NIST) guidance.

However, in October 2002, when the Computer Security Material Weakness Action Plan was developed and the goal of certifying 75% of its systems was established, the best available inventory consisted of 300 systems and applications. The IRS used this inventory as a baseline to measure progress toward achieving its goal. The IRS surpassed this goal and certified 82% of its inventory as of September 30, 2003. The IRS' systems inventory, the certification and accreditation approach, and material weakness goal were based on the guidance and criteria in place at that time and pre-dated the enactment of the Federal Information Security Management Act (FISMA) and the Expanding E-Government Scorecard for Information Technology Security under the President's Management Agenda. It is within this context that the IRS believes that it has satisfactorily completed the original actions outlined in the Computer Security Material Weakness Action Plan and that the existing material weakness should be closed.

b) During 2003, there were many changes that impacted systems certification and accreditation in the federal government. For example, during this time, the Department of the Treasury and OMB were implementing the FISMA which required the IRS to implement several changes to its Security Program. A key aspect of the changes was a new practical and cost effective certification and accreditation approach that will be fully compliant with FISMA, OMB, and NIST guidance. This new approach required that the IRS revisit the way it categorizes and counts its computer systems and applications. As a result, the IRS reviewed and revised its list of systems and applications, grouping these into General Support Systems, major applications, and other applications, to be consistent with OMB A-130 guidance. This effort was coordinated with Department of the Treasury and the revised listing of systems and applications was forwarded to OMB. Both the Department of the Treasury and OMB have endorsed the IRS' efforts to more accurately report its systems inventory and the IRS' new certification and accreditation approach. The IRS is well underway to achieve full certification and accreditation for all applicable systems and applications by early to mid-2005.

While the draft audit report is silent on whether the new IRS' certification and accreditation approach should be designated a new material weakness, the IRS will assess whether it is prudent to designate the approach as a material weakness and apply the new metric cited under the Expanding E-Government Scorecard for Information Technology Security under the President's Management Agenda, which states that at least 90 percent of systems should be certified and accredited for agencies to receive "green" status. The Chief, Mission Assurance, will brief the IRS' Financial and Management Controls Executive Steering Committee in September 2004 on whether the IRS' new certification and accreditation approach should be designated a material weakness.

**IMPLEMENTATION DATE:**

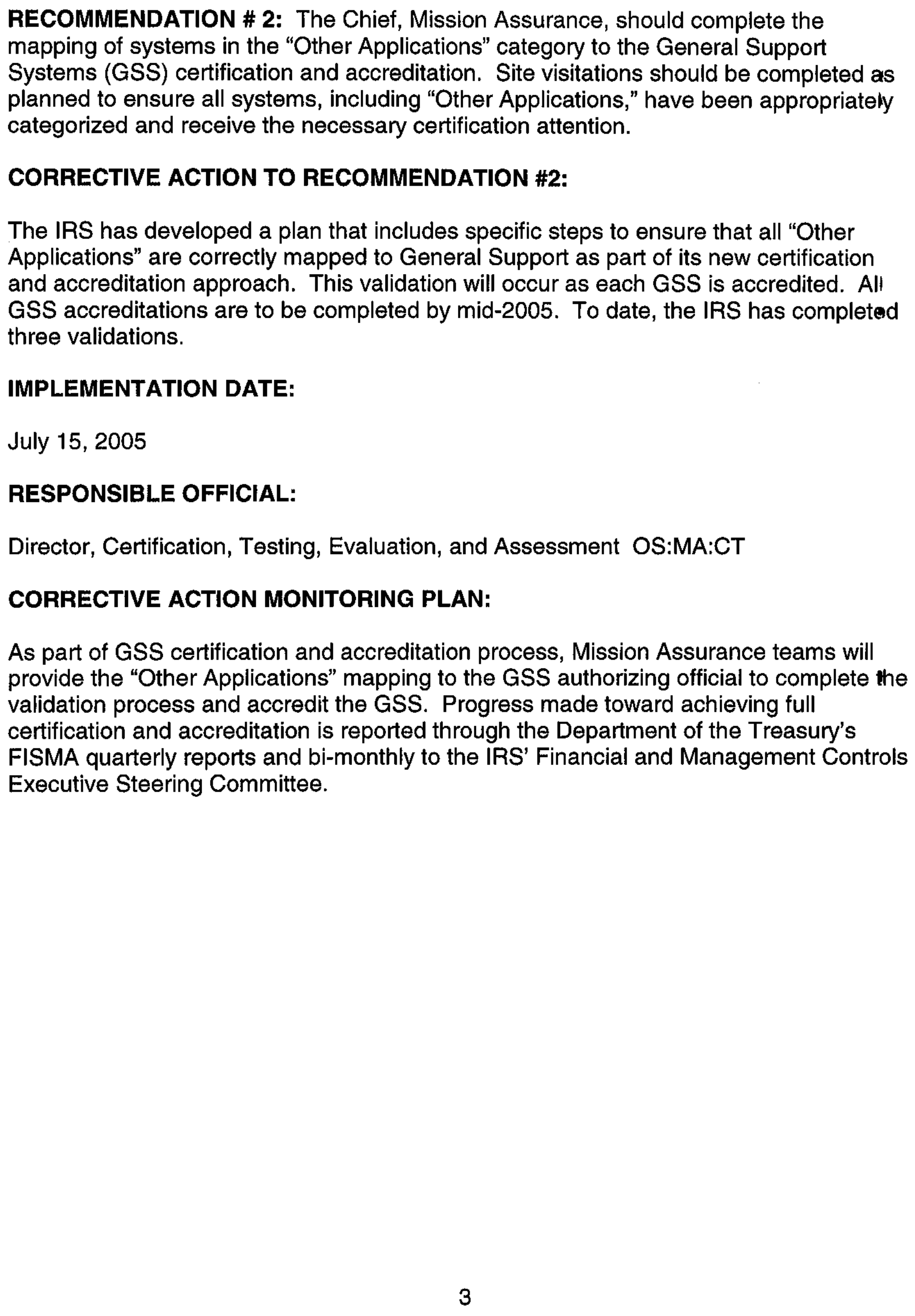
a) Completed. September 30, 2003
b) September 30, 2004

**RESPONSIBLE OFFICIAL:**

a) Director, Certification, Testing, Evaluation, and Assessment OS:MA:CT
b) Director, Certification, Testing, Evaluation, and Assessment OS:MA:CT

**CORRECTIVE ACTION MONITORING PLAN:**

The IRS developed a plan to achieve full certification and accreditation for all applicable systems and applications. Status meetings will be conducted periodically to identify problems and resolve issues related to the certification and accreditation effort. Progress made toward achieving full certification and accreditation is reported through Department of the Treasury's FISMA quarterly reports and bi-monthly to the IRS' Financial and Management Controls Executive Steering Committee.



**RECOMMENDATION # 2:** The Chief, Mission Assurance, should complete the mapping of systems in the "Other Applications" category to the General Support Systems (GSS) certification and accreditation. Site visitations should be completed as planned to ensure all systems, including "Other Applications," have been appropriately categorized and receive the necessary certification attention.

**CORRECTIVE ACTION TO RECOMMENDATION #2:**

The IRS has developed a plan that includes specific steps to ensure that all "Other Applications" are correctly mapped to General Support as part of its new certification and accreditation approach. This validation will occur as each GSS is accredited. All GSS accreditations are to be completed by mid-2005. To date, the IRS has completed three validations.

**IMPLEMENTATION DATE:**

July 15, 2005

**RESPONSIBLE OFFICIAL:**

Director, Certification, Testing, Evaluation, and Assessment OS:MA:CT

**CORRECTIVE ACTION MONITORING PLAN:**

As part of GSS certification and accreditation process, Mission Assurance teams will provide the "Other Applications" mapping to the GSS authorizing official to complete the validation process and accredit the GSS. Progress made toward achieving full certification and accreditation is reported through the Department of the Treasury's FISMA quarterly reports and bi-monthly to the IRS' Financial and Management Controls Executive Steering Committee.

**RECOMMENDATION # 3:** The Chief, Mission Assurance, should establish a formal process to monitor accreditations and report noncompliance, as needed, to the Deputy Commissioners to ensure accreditations are completed.

**CORRECTIVE ACTION TO RECOMMENDATION #3:**

Mission Assurance has implemented a process that will require all accreditation memoranda to be returned to Certification, Testing, Evaluation, and Assessment to complete the IRS' accreditation files. Additionally, as part of the 2004 FISMA reviews, the IRS will ensure that all accreditation memoranda are completed. Mission Assurance will provide the IRS Deputy Commissioners with a report of systems and applications whose accreditation memoranda are not in compliance at the end of the FISMA review cycle and yearly thereafter.

**IMPLEMENTATION DATE:**

November 15, 2004

**RESPONSIBLE OFFICIAL:**

Director, Certification, Testing, Evaluation, and Assessment OS:MA:CT

**CORRECTIVE ACTION MONITORING PLAN:**

Initial status reports will be provided upon completion of the 2004 FISMA effort and yearly thereafter.