



*Annual Assessment of the Internal Revenue
Service Information Technology Program*

September 29, 2011

Reference Number: 2011-20-106

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.

Phone Number | 202-622-6500

Email Address | TIGTACommunications@tigta.treas.gov

Web Site | <http://www.tigta.gov>



HIGHLIGHTS

ANNUAL ASSESSMENT OF THE INTERNAL REVENUE SERVICE INFORMATION TECHNOLOGY PROGRAM

Highlights

**Final Report issued on
September 29, 2011**

Highlights of Reference Number: 2011-20-106
to the Internal Revenue Service Chief
Technology Officer.

IMPACT ON TAXPAYERS

The Internal Revenue Service (IRS) relies extensively on its computer systems to carry out the responsibilities of administering our Nation's tax laws. As such, it must ensure its computer systems are effectively secured to protect financial and taxpayer data. The IRS also needs to ensure that it leverages technological advances to update its computer operations and improve customer satisfaction and that the computer systems supporting tax administration continue to operate efficiently and effectively.

WHY TIGTA DID THE AUDIT

This audit was initiated as part of TIGTA's Fiscal Year 2011 Annual Audit Plan and addresses the major management challenges of Security and Modernization. TIGTA annually assesses and reports on the adequacy and security of IRS information technology, as required by the IRS Restructuring and Reform Act of 1998.

WHAT TIGTA FOUND

The Business Systems Modernization Program (Modernization Program) is a complex effort to modernize IRS technology and related business practices. It involves integrating thousands of hardware and software components while replacing outdated technology and maintaining the current tax system. The IRS would not be able to deliver the Modernization Program without the support of the Cybersecurity and Enterprise Operations organizations.

The IRS's Fiscal Year 2011 financial plan for its Information Technology Program and operations remained relatively flat from its Fiscal Year 2010 budget of \$1.8 billion. The Fiscal Year 2011 financial plan included about \$264 million to go towards the Modernization Program. As of July 2011, the Modernization and Information Technology Services organization employed over 7,300 individuals.

Since last year's assessment, significant systems have been developed and implemented to improve the tax return processing environment, and additional improvements and upgrades are being developed and implemented. As such, TIGTA supports the IRS's request to downgrade the Modernization Program material weakness. However, computer security remains a material weakness, and the IRS needs to continue its emphasis and attention on becoming a security-conscious organization.

TIGTA also noted that the information technology operations program has implemented best practice principles, such as the Information Technology Infrastructure Library, designed to improve efficiency and effectiveness, and has taken action to improve the energy efficiency of its desktop computer equipment. While TIGTA is encouraged by these actions, the IRS has opportunities for making improvements and measuring its results.

WHAT TIGTA RECOMMENDED

Because this was an assessment report of the IRS's Information Technology Program through Fiscal Year 2011, TIGTA did not offer any recommendations. IRS officials were provided an opportunity to review and comment on the report.



TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 29, 2011

MEMORANDUM FOR CHIEF TECHNOLOGY OFFICER

Michael R. Phillips

FROM:

Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT:

Final Audit Report – Annual Assessment of the Internal Revenue
Service Information Technology Program (Audit # 201120003)

This report presents the results of our annual assessment of the Internal Revenue Service (IRS) Information Technology Program. The overall objective of this review was to assess the status of the IRS's Information Technology Program since June 2010, as required by the IRS Restructuring and Reform Act of 1998.¹ This review is part of our Fiscal Year 2011 Annual Audit Plan and addresses the major management challenges of Security and Modernization.

Copies of this report are also being sent to the IRS managers affected by the report findings. Please contact me at (202) 622-6510 if you have questions or Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services), at (202) 622-5894.

¹ Pub. L. No. 105-206, 112 Stat. 685 (codified as amended in scattered sections of 2 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.).



*Annual Assessment of the Internal Revenue Service
Information Technology Program*

Table of Contents

BackgroundPage 1

Results of ReviewPage 4

 Modernization Program BackgroundPage 4

 The Modernization Program Continues to Deliver Business Value
 and Benefits to Taxpayers.....Page 4

 The Modernization Program Demonstrates Improvements in
 Delivering Planned CapabilitiesPage 7

 The Modernization Program Addressed Process
 and Control WeaknessesPage 11

 Information Security Background.....Page 13

 Some Progress Is Being Made to Improve Information SecurityPage 14

 Continued Emphasis and Attention Is Needed to Allow the Internal
 Revenue Service to Become a Security-Conscious OrganizationPage 18

 Information Technology Operations BackgroundPage 20

 The Information Technology Operations Program Has Improved
 Its Efficiency and Effectiveness.....Page 20

Appendices

 Appendix I – Detailed Objective, Scope, and MethodologyPage 26

 Appendix II – Major Contributors to This ReportPage 28

 Appendix III – Report Distribution ListPage 29

 Appendix IV – Listing of Treasury Inspector General for Tax
 Administration Reports Reviewed.....Page 30

 Appendix V – Project Cost and Schedule Variances.....Page 33

 Appendix VI – Glossary of Terms.....Page 34



*Annual Assessment of the Internal Revenue Service
Information Technology Program*

Abbreviations

CADE	Customer Account Data Engine
FY	Fiscal Year
IBM	International Business Machines Corporation
IRS	Internal Revenue Service
MeF	Modernized e-File
MITS	Modernization and Information Technology Services
TIGTA	Treasury Inspector General for Tax Administration



*Annual Assessment of the Internal Revenue Service
Information Technology Program*

Background

The Internal Revenue Service (IRS) Restructuring and Reform Act of 1998¹ requires the Treasury Inspector General for Tax Administration (TIGTA) to annually evaluate the adequacy and security of the IRS Information Technology Program. This report provides our assessment of the IRS's Information Technology Program and operations.

As of July 2011, the Modernization and Information Technology Services (MITS) organization employed over 7,300 individuals. Figure 1 provides a breakdown of MITS employees by their respective business unit functions.

Figure 1: Number of MITS Employees by Business Unit
(in descending order)

MITS Business Unit	Number of Employees
Applications Development	2,397
Enterprise Operations	1,748
End Users Equipment & Services	1,295
Enterprise Networks	510
Cybersecurity	410
Enterprise Services	287
Strategy & Planning	270
Affordable Care Act – Program Management Office	267
Management Services	73
Customer Account Data Engine Program Management Office	68
Equal Employment Opportunity and Diversity	7
Deputy Chief Information Officer for Strategy/Modernization	4
Deputy Chief Information Officer for Operations	3
TOTAL	7,339

Source: Treasury Integrated Management Information System as of July 2011.

¹ Pub. L. No. 105-206, 112 Stat. 685 (codified as amended in scattered sections of 2 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.).



Annual Assessment of the Internal Revenue Service Information Technology Program

The IRS's Fiscal Year (FY) 2011 financial plan for its Information Technology Program and operations remained relatively flat from its FY 2010 budget of \$1.8 billion. In addition, the FY 2011 financial plan included about \$264 million to go towards the Business Systems Modernization Program (Modernization Program).

While the IRS's Modernization Program encompasses dozens of projects and systems, the core projects that the IRS refers to as the "Pillars of Modernization" are the:

- Current Customer Account Data Engine (CADE) and CADE 2² – the databases and related applications that include applications for daily posting, settlement, maintenance, refund processing, and issue detection for taxpayer tax account and return data.
- Modernized e-File (MeF) – an electronic filing platform used for electronic filing of tax returns for both business and individual taxpayers.
- Account Management Services/Integrated Data Retrieval System – systems that provide IRS employees with the ability to view, access, update, and manage taxpayer accounts.

The IRS would not be able to deliver these core projects without the support of the Cybersecurity and Enterprise Operations organizations. The Cybersecurity organization is responsible for ensuring the IRS's compliance with Federal statutory, legislative, and regulatory requirements governing measures to assure the confidentiality, integrity, and availability of IRS electronic systems, services, and data. The Enterprise Operations organization supports the MITS organization by providing efficient, cost-effective, secure, and highly reliable computing (mainframe and server) services for all IRS business entities and taxpayers.

In March 2010, Congress enacted legislation that will significantly impact the work performed by the MITS organization. The Patient Protection and Affordable Care Act³ was signed into law and later amended on March 30, 2010, by the Health Care and Education Reconciliation Act⁴ (hereafter referred to as the Affordable Care Act). At least 42 provisions add to or amend the Internal Revenue Code, and at least 8 require the MITS organization to build new processes that do not exist in current tax administration. The IRS realized the vastness of the work required by the Affordable Care Act and, in June 2010, created a new organization called the Associate Chief Information Officer Affordable Care Act – Program Management Office (hereafter called the Program Management Office) to mitigate any impact to its ongoing development efforts and to ensure successful delivery of the required new systems. The Program Management Office will be accountable for achieving the defined goals and for managing and integrating the required components, including building new services and applications, enhancing and extending existing applications, and ensuring that the appropriate governance and control processes are followed throughout implementation.

² See Appendix VI for a glossary of terms.

³ Pub. L. No. 111-148, 124 Stat. 119 (2010).

⁴ Pub. L. No. 111-152, 124 Stat. 1029.



*Annual Assessment of the Internal Revenue Service
Information Technology Program*

The compilation of information for this report was conducted at the TIGTA office in Atlanta, Georgia, during the period May through July 2011. The information presented in this report is derived from TIGTA audit reports issued since June 2010. We also reviewed relevant Government Accountability Office reports relating to IRS information technology issues. These previous audits and our analyses were conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. One of our audits is on the Federal Information Security Management Act.⁵ For this review, we conduct an annual independent evaluation of information security policies, procedures, and practices as well as evaluate compliance with Federal Information Security Management Act requirements. We believe that the evidence obtained provides a reasonable basis for our finding and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II. A listing of the audit reports used in this assessment is presented in Appendix IV.

⁵ 44 United States Code (U.S.C.) sections (§§) 3541–3549.



Annual Assessment of the Internal Revenue Service Information Technology Program

Results of Review

Modernization Program Background

For FY 2011, the TIGTA cited that modernization of IRS technology and business processes was the second top challenge for the IRS. The Modernization Program is a complex effort to modernize IRS technology and related business processes. It involves integrating thousands of hardware and software components while replacing outdated technology and maintaining the current tax system. The Modernization Program receives separate funding from Congress. Since its inception in FY 1999, the IRS has received over \$3 billion. The IRS projected it needed \$334 million for the Modernization Program in its FY 2012 budget request.

Factors that characterize the IRS's complex information technology environment include widely varying inputs from taxpayers (from simple concise records to complex voluminous documents), seasonal processing with extreme variations in processing loads, transaction rates on the order of billions per year, and data storage measured in trillions of bytes. The Modernization Program is working toward providing improved benefits to taxpayers that include:

- Issuing refunds, on average, 5 days faster than existing legacy systems.
- Offering electronic filing capability for individuals, large corporations and small businesses, tax-exempt organizations, and partnerships, with dramatically reduced processing error rates.
- Delivering web-based services for tax practitioners, taxpayers, and IRS employees.
- Providing IRS customer service representatives with faster and improved access to taxpayer account data with real-time data entry, validation, and updates of taxpayer addresses.

The Modernization Program Continues to Deliver Business Value and Benefits to Taxpayers

Data and technology are central to the future of tax administration. The IRS is on schedule to deliver the CADE 2 system for the 2012 Filing Season. Completion of the CADE 2 system is the cornerstone of IRS information technology modernization that will expedite refunds to millions of individual taxpayers. It is also a prerequisite for other major initiatives, such as expansion of online paperless services. The ability of the IRS to support increasingly complex taxpayer service and compliance initiatives will be severely limited until the new taxpayer account database is completed. IRS modernization efforts continue to focus on core tax



Annual Assessment of the Internal Revenue Service Information Technology Program

administration systems designed to provide more sophisticated tools to taxpayers and to IRS employees. The Modernization Program has continued to provide new information technology capabilities and the related benefits to both the IRS and taxpayers. Since January 2011, the IRS has implemented new versions of the current CADE and MeF systems and the Account Management Services system. Additionally, the IRS has continued making progress in preparing for the deployment of the CADE 2 system.

Current Customer Account Data Engine

The current CADE system is a component of the Modernization Program. It consists of modernized databases and related applications that work in conjunction with the IRS Master File System. Current CADE Release 6.2 was deployed in January 2011 to incorporate Tax Year 2010 tax law changes affecting individual taxpayers and to provide technical improvements to the infrastructure and availability of the CADE system. From January through May 2011, the current CADE system processed over 39.9 million tax returns and issued more than 35.1 million refunds totaling in excess of \$65.6 billion.

The current CADE system is in the process of transferring accounts back to the IRS Master File in preparation for the transition to the CADE 2 system. As of May 2011, the IRS migrated over 69 million accounts and was on track to complete the migration process by the end of June 2011. Once the migration of the current CADE to CADE 2 system is complete, the current CADE system will be taken offline.

Customer Account Data Engine 2

The CADE 2 Program is the top information technology modernization project in the IRS. The CADE 2 strategy involves three phases:

Transition State 1. Modifies the Individual Master File from a weekly cycle to daily processing, establishes a new relational database to store all individual taxpayer account information, and provides management tools to more effectively use data for compliance and customer service. The IRS plans to implement Transition State 1 in January 2012.

Transition State 2. Launches a single processing system where applications directly access and update the taxpayer account database. It will continue efforts toward addressing previously identified financial material weaknesses. The IRS plans to implement Transition State 2 in January 2014. During a June 16, 2011, meeting with IRS Modernization executives, the TIGTA learned that a lack of funding may delay delivery of this phase. The IRS is working to identify funding it could use to begin high-level planning efforts.

Target State. Consists of a single system using elements of the Individual Master File and the current CADE system, eliminating all transitional applications used to link the



Annual Assessment of the Internal Revenue Service Information Technology Program

current CADE system, Individual Master File, and the Integrated Data Retrieval System. The complete solution is also planned to address all the financial material weaknesses. As of April 28, 2011, the IRS had not established a Target State implementation date.

The IRS established the CADE 2 Program Management Office to provide state-of-the-art individual taxpayer account processing and technologies to improve service to taxpayers. The CADE 2 Program Management Office plans to create a modernized processing environment where applications both access and update an authoritative relational database to manage all individual taxpayer accounts. To assist in this effort, the IRS established two systems development projects (Daily Processing and Database Implementation) and completed several prototypes. The objective of each prototype was to demonstrate confidence in the CADE 2 approach by verifying system viability and performance and defining components to serve as the foundation for development activities.

With the “go-live” date for Transition State 1 fast approaching, the IRS continues to work on ensuring the CADE 2 system is successfully deployed by dividing the processing framework into manageable segments. The IRS also developed a set of guiding principles that will help enable a seamless and successful “go live” and post-implementation support for Transition State 1. Some of these principles include:

- Ensuring the most critical components with the highest impact/risk are prioritized in order to increase the likelihood of overall project success.
- Including people, processes, and technology in discussions about change.
- Establishing a central readiness team to monitor progress and ensure key messages are consistently communicated throughout the organization.

Modernized e-File

The MeF system streamlines tax return filing processes and reduces the costs associated with paper tax returns. The first phase of the MeF system (Release 6.1) for individual income tax returns included the U.S. Individual Income Tax Return (Form 1040), Application for Automatic Extension of Time to File U.S. Individual Income Tax Return (Form 4868), and 21 forms and schedules related to the Form 1040 for Tax Year 2009. The IRS first began accepting individual tax returns through the MeF system in February 2010.

The second phase of the MeF system (Release 6.2) for individual income tax returns was implemented during the 2011 Filing Season. Release 6.2 does not provide for the filing of any additional tax forms or schedules. The primary difference between the functionality of Releases 6.1 and 6.2 is the ability for individual taxpayers to file prior year tax returns. For example, for the 2011 Filing Season, individual taxpayers will be able to file both their Tax Years 2009 and 2010 tax returns using the MeF system.



Annual Assessment of the Internal Revenue Service Information Technology Program

Returns submitted through the MeF system have an average of 8 percent processing error rate, compared to 19 percent for transcription-based paper processing. As of May 31, 2011, the IRS accepted 9.8 million individual tax returns transmitted through the MeF system for processing, in addition to the 6.3 million corporate, partnership, and exempt organization returns and forms accepted. The third phase of the MeF system (Release 7.0) is planned for deployment in Fiscal Year 2012 and includes the rollout of over 125 remaining Forms 1040, including the Income Tax Return for Single and Joint Filers With No Dependents (Form 1040 EZ). The IRS plans to spend about \$67.2 million on this release of the MeF system.

Account Management Services

The Account Management Services system provides IRS employees with the tools to access information quickly and accurately in response to complex customer inquiries. The final Account Management Services system release, Release 2.1, provided all users (approximately 40,000) with the ability to view correspondence images online and on demand. Direct access to view images reduced case cycle time from 10–14 days to zero. In May 2011 alone, the Account Management Services system processed over 234,000 correspondence image view requests. The cumulative total of correspondence image view requests exceeded 2.7 million since its deployment in February 2010.

The Modernization Program Demonstrates Improvement in Delivering Planned Capabilities

The Modernization Program continues to help improve IRS operations and has demonstrated successes in improving business practices by implementing new information technology solutions. Management of project costs and schedule has shown a drastic improvement, but requirements development and management continues to need attention.

Process improvement activities

The IRS has a sophisticated Enterprise Life Cycle development process that it uses for large application development projects. However, this process contains several development phases (i.e., milestone reviews), can require extensive documentation, and may take several months to years to complete. Therefore, the IRS Enterprise Life Cycle Project Management Office is working within the applications development offices to develop more streamlined lifecycle processes for smaller, faster paced developments. For this reason, the MITS organization has taken steps to implement an iterative approach to its systems development activities.

The iterative path is an adaptive development approach in which projects start with initial planning and end with deployment, with repeated cycles of requirements discovery, development, and testing in between. This development path is well suited to projects and environments that change rapidly, because each iteration presents new opportunities for the



Annual Assessment of the Internal Revenue Service Information Technology Program

project to adapt to change. Some benefits of implementing the iterative path approach include streamlining the number of development phases, involving process owners and business stakeholders to continuously provide feedback, and prototyping (i.e., developing an early version of the solution to see if it meets needs).

During FY 2011, we conducted several audits of the IRS's systems development activities and found the IRS made progress adopting the iterative path.

- During our review to determine the effectiveness of the CADE 2 prototype efforts, we found that the CADE 2 Program Management Office created five prototype teams to demonstrate confidence in the CADE 2 solution by verifying system viability and performance and by defining components that will serve as the foundation for development activities. In addition, the prototype teams generally managed their objectives effectively and took steps to overcome risks identified during prototype planning.⁶
- During our review to determine whether the IRS adequately tested and secured the IRS2GO smartphone application, we determined the IRS2GO application adequately protects data transmissions and personally identifiable information. The IRS smartphone application provides tax tips to the smartphone user and allows the user to check on the status of his or her tax refund.⁷
- During our review to evaluate the MITS organization's planning effort to implement the Affordable Care Act, we identified that the Program Management Office implemented processes to ensure that the systems it develops meet the businesses needs by involving business unit representatives in the development and decisionmaking processes. We also found that the Program Management Office collaborates with its internal and external stakeholders. For example, the Program Management Office staff conducted periodic joint meetings with the internal stakeholders such as the following: the Large Business and International, Small Business/Self-Employed, and Tax Exempt and Government Entities Divisions. Topics of discussions include requests for approval to use a particular development process and approval to begin projects and action items such as working to minimize the impact to filing season projects.⁸

Modernization Program cost and schedule management

In our FY 2010 assessment of the Modernization Program,⁹ we reported that 3 (38 percent) of the 8 project milestones were not delivered within the accepted 10 percent variance in schedule.

⁶ See Appendix IV, Number 4.

⁷ See Appendix IV, Number 23.

⁸ See Appendix IV, Number 25.

⁹ See Appendix IV, Number 3.



Annual Assessment of the Internal Revenue Service Information Technology Program

This fiscal year, the IRS delivered all 7 of its projects milestones on time and almost all were completed within the accepted 10 percent variance for cost. The exception to this was for MeF Release 7. This project experienced a 24 percent cost variance.

Appendix V presents the cost and schedule variance for Modernization Program project releases delivered from October 2010 through June 2011.

Some systems development disciplines continue to need attention

During the past year, the TIGTA reported on the adequacy of the development and management of the Modernization Program and other modernization project requirements. These issues included adequacy of controls for managing the development of requirements, documentation and controls over requirements testing and traceability, and updating project work breakdown schedules. These issues were present in five Modernization Program reports on the CADE 2 Program and the MeF Program.

CADE 2 Prototypes – The CADE 2 Program Management Office took steps to formulate and initiate prototype efforts. These steps included development of program guidance and prototype processes and steps to identify and manage risks related to the prototyping efforts. Further, the CADE 2 Program Management Office took actions to monitor and evaluate progress in accomplishing the prototype objectives. However, some of the prototype teams did not initially document test plans, test results, and issues logs. Without these documents, relevant business requirements needed for testing may be omitted, there may not be sufficient evidence to show all necessary requirements were tested, and similar issues could recur.¹⁰

CADE 2 Program Management Office – The CADE 2 Program Management Office was established with a mission to provide state-of-the-art individual taxpayer account processing and technologies to improve service to taxpayers and enhance IRS tax administration. The CADE 2 Program Management Office issued guidelines for key systems development processes and convened numerous meetings to provide oversight for the work being performed. As status meetings were convened, it became evident to CADE 2 Program Management Office officials there was a significant challenge involved in assembling diverse processes into a comprehensive set of activities that would be well understood and consistently applied across the Program and the projects. While Program guidelines specified the systems development procedures, the guidelines and the actual processes performed by the project teams were not always consistent. For example, the CADE 2 Program Management Office did not initially have a Program Test Plan and, as a result, experienced multiple delays in its development during the course of our review. If the CADE 2 project teams do not receive sufficient guidance on developing their test plans, the CADE 2 system may not be properly tested and the system may not work as intended

¹⁰ See Appendix IV, Number 4.



*Annual Assessment of the Internal Revenue Service
Information Technology Program*

when deployed into IRS operations. During the course of our review, the IRS developed the required Program Test Plan.¹¹

CADE 2 Daily Processing – The CADE 2 Daily Processing project is not a new application development project. Instead, it will enhance the existing IRS Master File, currently processing on a weekly schedule, and make it daily processing. By moving to daily processing, the CADE 2 Daily Processing project will provide immediate and obvious benefits, including faster refunds to taxpayers, faster posting of payments, and more efficient adjustments to taxpayer accounts.

Our review determined the CADE 2 Daily Processing project has steadily progressed from project initiation (Milestone 1) through Physical Design (Milestone 4a). As a result, the IRS is closer to achieving one of its modernization goals, daily processing of taxpayer accounts. However, the CADE 2 Daily Processing business rules were not gathered and completed as required and were still being developed after the December 2010 Milestone 3 exit. For example, when the Milestone 3 exit occurred, the business rule that determines eligibility of accounts for daily processing was not developed. Additionally, prior to the Milestone 4a exit, 16 business rules were not written as required by the Enterprise Life Cycle. The risk of incomplete business rules could contribute to untraced requirements, which may adversely impact systems design and testing activities.¹²

CADE 2 Database Implementation – As part of the CADE 2 Transition State 1, the IRS established the Database Implementation project to move it away from operating in two tax processing environments and to maintain a single system of record for all individual taxpayer accounts. The primary deliverable of the CADE 2 Database Implementation project is a relational database that will house individual taxpayer account data, currently being processed by the IRS Master File and current CADE system. The CADE 2 Database Implementation team made progress towards implementing this new project and providing IRS employees with the ability to view updated taxpayer account information online. However, the work breakdown structure used to define and group project tasks and define the scope of the project was not comprehensive in including all activities through Milestone 5.¹³

MeF – In our report on the development of MeF Release 6.2, we reported that improvements are needed for tracking performance issues. Specifically, internal matrices captured performance enhancements; however, there was either inadequate or no support documentation for performing and tracking work or for showing that necessary corrective action was taken. As a result, the TIGTA was unable to validate whether captured performance elements identified during the 2010 Filing Season were ever resolved. In addition, the IRS did not follow the MeF Risk Management Plan, which requires all issues and candidate risks to be entered into the Item Tracking Reporting and Control System to ensure monitoring and control by external

¹¹ See Appendix IV, Number 9.

¹² See Appendix IV, Number 7.

¹³ See Appendix IV, Number 8.



Annual Assessment of the Internal Revenue Service Information Technology Program

stakeholders. During our review of the administration and oversight of the MeF Program, we identified several issues and risks that the IRS did not properly track. The lack of adherence to guidance negatively impacts the IRS's ability to efficiently monitor and track issues that are critical for external stakeholder awareness.¹⁴

We also recently completed an audit to determine whether individual income tax returns will be accurately and timely processed and whether sufficient progress is being made to replace the Legacy e-File system for individual tax returns in the 2013 Filing Season. We reported that processes used to test and monitor the MeF system do not ensure MeF system business rules designed to validate basic requirements on a tax return are working as intended. As a result, the IRS continues to have limited assurance that the MeF system is accurately processing individual tax returns. Ineffective or insufficient monitoring of tax return processing increases the risk that tax returns processed through the MeF system will be erroneously accepted or rejected. This risk will grow significantly as the volume of tax returns processed through the MeF system increases and the types of forms and schedules are expanded. In addition, lower than expected tax return transmitter participation and tax return volumes raise significant concern regarding the IRS's ability to fully replace the Legacy e-File system for the 2013 Filing Season.¹⁵

The Modernization Program Addressed Process and Control Weaknesses

In last year's assessment report, we reported that the IRS had plans to refocus the Modernization Program, especially as it related to CADE 2 Program activities. At that time, we believed the IRS should continue to consider the overall Modernization Program as a material weakness until it could demonstrate success with the CADE 2 system. In response to our report, IRS management commented the IRS is at a key point in the Modernization Program and is well on the way to successfully demonstrating that the CADE 2 system can operate securely and effectively.

When the IRS agreed to declare the Modernization Program as a material weakness in Calendar Year 1995, it set up an Action Plan that listed all of the management and control weaknesses that needed improvement. The goal of the Action Plan was to "improve IRS modernization management controls and processes to consistently improve delivery of systems with expected functionality within budget and on time that will dramatically improve both internal operations and services to taxpayers." The Action Plan included identifying gaps and weaknesses, establishing corrective actions, monitoring progress, and identifying continuous improvement opportunities.

¹⁴ See Appendix IV, Number 6.

¹⁵ See Appendix IV, Number 28.



Annual Assessment of the Internal Revenue Service Information Technology Program

The key indicators used to evaluate the progress on the Action Plan are: effective management processes will be delivery of systems on time and within budget (variance of less than 10 percent for estimates of the next Milestone at the prior Milestone exit); no significant decrease in functionality; and relatively clean management process audits from the TIGTA and from the review of the Modernization Annual Expenditure Plan by the Government Accountability Office. Management processes include risk management, configuration management, cost and schedule estimating, management reporting, human capital management, Enterprise Life Cycle, and several other agreed-to management processes as reported every month by the IRS.

In addition to the Action Plan, the IRS instituted a program to monitor action plans built on the Capability Maturity Model Integration¹⁶ framework for the control weaknesses that needed improvement to ensure they were managed in accordance with agreed metrics. At the request of the IRS, we completed work to determine whether the Applications Development function's Quality Assurance Program Office ensures development projects implement a coordinated set of activities that conform to organizational policies, processes, and procedures that meet the standards of Capability Maturity Model Integration – Development maturity level 2.¹⁷ We found the Internal Revenue Manual included the quality assurance requirements. Further, the Quality Assurance Program Office's processes, guidance, and procedures generally meet the requirements for quality assurance. In addition, qualified specialists were employed to perform audits to determine the level of compliance with the organizational standards, processes, and procedures, and feedback was provided to project staff and managers on the results of the quality assurance activities. The Quality Assurance Program Office met the annual audit plan goals in FYs 2008 and 2009 by performing 65 audits and 79 audits, respectively. The IRS received external accreditation for maturity level 2 in November 2010, indicating that the Applications Development function exhibits a managed level of maturity with basic project management capability focus in key process areas. The IRS plans to achieve maturity level 3 (a more "defined" level of maturity with process standardization) in FY 2013.

During FY 2011, the Chief Technology Officer and other MITS executives met with the TIGTA to request support to downgrade the IRS's Modernization Program material weakness. The MITS organization's position is that the IRS has met all of the conditions and completed all management and control improvements from the original and revised action plans the IRS defined to resolve the material weakness. In its June 2011 request letter to the Department of the Treasury, IRS management cited several key accomplishments, such as implementing a high-priority initiative process to address ongoing improvements, implementing the previously discussed Capability Maturity Model Integration framework, and sustaining performance delivering systems on time and within budget (see the prior section on cost and schedule management).

¹⁶ The Capability Maturity Model Integration defines industry best practices for management software development projects as set forth by industry experts.

¹⁷ See Appendix IV, Number 5.



Annual Assessment of the Internal Revenue Service Information Technology Program

The TIGTA has been involved in audits of the Modernization Program since FY 2000, and we have seen the improvement in the management and controls of the program. While our audit reports have pointed out (and continue to do so) concerns and issues with the implementation of the management controls, overall we have seen significant progress in the management of the Modernization Program. Significant systems such as the CADE 2, Account Management Services, and MeF systems have been developed and rolled out to improve the tax return processing environment, and additional improvements and upgrades are being developed and implemented.

As such, we concur that the IRS has substantially completed the improvement items listed in the Action Plan and has met the indicators used to evaluate its progress. We would support the request to downgrade the Modernization Program from a material weakness to a deficiency. This does not mean that the Modernization Program no longer has concerns and issues, but the improvements put in place (and reviewed by the TIGTA and the Government Accountability Office) have generally improved the management of the Modernization Program. We would suggest that the IRS consider the Modernization Program to be a high-risk area and continue to stress improvements in processes and performance. IRS management indicated that once the Modernization Program achieves Capability Maturity Model Integration maturity level 3, it will seek to close this deficiency.

Information Security Background

The IRS relies extensively on its computer systems to carry out the demanding responsibilities of administering our Nation's tax laws, including the processing of Federal tax returns. According to the *IRS Data Book, 2010*, the IRS received more than 230 million tax returns, of which 141 million returns were from individual taxpayers. As computer usage continues to be inextricably integrated into the IRS's core business processes, the need for effective information system security becomes essential to ensure that data is protected against inadvertent or deliberate misuse, improper disclosure, or destruction and that computer operations supporting tax administration are secured against disruption or compromise.

The IRS, like all other Federal Government entities, faces the daunting task of securing its computer systems against the growing threats of cyber attacks. According to the Office of Management and Budget's FY 2010 report to Congress on the implementation of the Federal Information Security Management Act, the number of cyber incidents affecting United States Federal agencies shot up 39 percent in FY 2010 when Federal agencies reported 41,776 cyber attacks. More recently in July 2011, the Pentagon acknowledged a serious data breach when a Department of Defense contractor suffered "one of its largest cyber attacks ever" when what it believes to be a foreign government stole 24,000 files containing sensitive data. Lastly, a July 2011 report from the National Security Council warns that international cybercrime has reached the upper echelon of threats to the security of the United States and poses a significant threat to sensitive corporate and government computer networks.



Annual Assessment of the Internal Revenue Service Information Technology Program

For FY 2011, the TIGTA cited that “*Securing the IRS*” was the top management challenge for the IRS. This priority designation was given due to increasing threats, both cyber and physical, against the IRS and the potentially expanding role of the IRS. Animosity towards tax collection is nothing new, though the threat vector has increased recently. For the IRS, the threat became reality when, in February 2010 in Austin, Texas, a disgruntled taxpayer flew his small aircraft into a building partially occupied by the IRS with the intent of killing as many IRS employees as possible.

Some Progress Is Being Made to Improve Information Security

The Cybersecurity organization within the MITS organization has primary responsibility for guiding the IRS in its efforts to protect computer systems and sensitive data and is responsible for ensuring the IRS’s compliance with Federal statutory, legislative, and regulatory requirements governing measures to assure the confidentiality, integrity, and availability of IRS electronic systems, services, and data. The Cybersecurity organization provides management and oversight for the IRS Information Technology Security Program. Its mission is to assure the security and resilience of information technology systems and data by providing solutions to the security risks encountered by business customers. The security environment in which the IRS operates is constantly changing. Third-party communications and new centers of communication have merged to challenge the outdated environment formed more than a half a century ago. Nevertheless, close collaboration and cooperation with all organizations remain crucial to meeting the IRS’s strategic goals.

The IRS is making some progress over information security and continues to place a high priority on efforts to improve its information security program. For example, in the IRS’s Strategic Plan for FYs 2009 to 2013, one of the major trends affecting the IRS is the “*explosion in electronic data, online interactions, and related security risks.*” Another example of the IRS’s commitment toward information security is the IRS’s Information Technology Security Program Plan, issued in September 2009. The Information Technology Security Program Plan is designed to enhance collaboration, provoke thought and comment, and guide all security efforts across the IRS community. In addition, the Plan serves as a roadmap and a basis for benchmarking information security performance toward attaining security objectives. Lastly, senior leaders of the IRS will be able to use the Security Program Plan as input to their strategic business planning process.

During FY 2011, we conducted several audits on information security and found the IRS is taking steps for securing technology.

- During our review to determine whether IRS controls, policies, and procedures for sensitive email messages to taxpayers adequately protected taxpayer data, we found the IRS is using email to enhance customer service and provide a more expedient and efficient way to exchange information. In addition, the IRS has effective controls to



*Annual Assessment of the Internal Revenue Service
Information Technology Program*

remove email accounts from the email system when the employee separates from the IRS. In FY 2010, the IRS conducted monthly security assessments of its email servers.¹⁸

- During our review to evaluate security over the IRS's use of wireless technologies and the IRS's development of a smartphone application, IRS2GO, we found security configurations were generally in place and working as intended.¹⁹
- During our review to evaluate whether the IRS implemented access controls on its Automated Insolvency System, we found the IRS established access controls, such as automatic system lockout after three unsuccessful login attempts, good password requirements, and restricting database access to only database administrators, which limits who has access to the systems.²⁰
- During our review²¹ to evaluate whether the CADE 2 Program Management Office planned and provided oversight for Transition State 1 design activities, we found that the IRS planned enhanced security controls for the CADE 2 system and the Cybersecurity organization was heavily engaged and proactive in its assigned role of managing all aspects of CADE 2 system security. In addition, the IRS contracted with an independent firm to complete a threat susceptibility analysis on the CADE 2 Transition State 1. The contractor's report concluded that threats to the CADE 2 Transition State 1 by external interfaces and databases appear to be minimal.²²
- During our review to determine whether adequate security controls have been established for the International Business Machines Corporation (IBM) DB2 databases running on the IBM z/OS operating system, we reviewed two applications (the Electronic Tax Administration Marketing Database and the Tax Return Database) owned by the Wage and Investment Division that share resources on the IBM mainframe to verify that the implementation of these applications met IRS standards. Our analysis of system files and system-generated reports verified that both applications met the IRS configuration and security standards for the IBM z/OS operating system and the DB2 database.²³

However, computer security remains the top management challenge and continued vigilance is needed to minimize security weaknesses throughout the IRS and ensure the IRS becomes a security-conscious organization.

¹⁸ See Appendix IV, Number 16.

¹⁹ See Appendix IV, Number 23.

²⁰ See Appendix IV, Number 18.

²¹ See Appendix IV, Number 9.

²² See Appendix IV, Number 7.

²³ See Appendix IV, Number 26.



*Annual Assessment of the Internal Revenue Service
Information Technology Program*

Computer security remains as a material weakness

The Federal Managers Financial Integrity Act of 1982²⁴ requires that each agency conduct annual evaluations of its systems of internal accounting and administrative controls and submit an annual statement on the status of the agency's system of management controls. In the event that an agency determines the existence of shortcomings in operations or systems which severely impair or threaten the organization's ability to accomplish its mission or to prepare timely and accurate financial statements, the Department of the Treasury directs the agency to declare a material weakness on that particular area.

In Calendar Year 1997, the IRS designated computer security as a material weakness. The computer security material weakness compromises the accuracy and availability of the IRS financial information and places sensitive information regarding IRS operations and taxpayers at risk. The IRS further categorized the computer security material weakness into nine components: (1) network access controls; (2) key computer applications and system access controls; (3) software configuration; (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.

According to the IRS, the IRS had closed or completed all planned actions for five of the nine components: (1) network access controls (completed in July 2010); (2) functional business, operating, and program unit security roles and responsibilities (completed in March 2009); (3) segregation of duties between system and security administrators (closed in September 2005); (4) security training (closed in October 2008); and (5) certification and accreditation (closed in October 2008).

Since June 2010, we conducted four audits related to the computer security material weakness. The IRS agreed with the findings below and provided adequate corrective actions to address our findings unless noted otherwise.

- During our review of enterprise audit trails, we reported that, while the IRS has taken several steps to improve its management of audit trails and has significantly increased its staffing and funding for FY 2010, substantial efforts and sustained funding are needed to address the audit trails portion of the computer security material weakness. We reviewed 20 major computer systems to determine the level of compliance with the IRS's audit trail policy and guidance and found that events were not being adequately captured and reviewed on many databases, applications, and operating systems because: (1) very few systems have audit plans, (2) the IRS did not have adequate event capturing and report

²⁴ Pub. L. No. 97-255 (31 U.S.C. §§ 1105, 1106, 1108, 1113, 3512).



*Annual Assessment of the Internal Revenue Service
Information Technology Program*

generating software tools, (3) audit reports were not being generated, and (4) the IRS determined that capturing required events could hurt system performance.²⁵

- During our review of the security roles and responsibilities component of the material weakness, we found the IRS completed the necessary work on two of the six corrective actions established to address this material weakness component. The other four corrective actions pertained to: (1) document information technology security roles and responsibilities, (2) develop and document day-to-day information technology security procedures and guidelines, (3) conduct compliance assessments to verify and validate security roles and responsibilities, and (4) establish metrics to measure successful operations. Although the IRS made progress in correcting previously reported information security weaknesses, lack of adherence to guidelines continues to jeopardize the confidentiality, integrity, and availability of financial and sensitive taxpayer information.²⁶
- During our review of the assessment of ongoing disaster recovery, we found the IRS completed or will complete many of the corrective actions to address the contingency planning and disaster recovery component of the material weakness. As a result, the IRS will be downgrading this component during FY 2011.²⁷
- During our review of the IRS's Federal Financial Management Improvement Act of 1996²⁸ remediation plans for the period of January to September 2009, we found the IRS has experienced difficulties in developing comprehensive remediation actions required to resolve noncompliance related to computer security and reliably estimating the resources and time necessary to implement remedial actions. Complete and reliable information is critical to the IRS's ability to accurately report on the results of its operations to both internal and external stakeholders, including taxpayers.²⁹

In addition, during May 2010 to March 2011, the Government Accountability Office assessed whether controls over key financial and tax processing systems are effective in ensuring the confidentiality, integrity, and availability of financial and sensitive taxpayer information in conjunction with its audits of the IRS's FY 2010 and 2009 financial statements. The Government Accountability Office found that the IRS did not consistently implement controls that were intended to prevent, limit, and detect unauthorized access to its financial systems and information. For example, the agency did not sufficiently (1) restrict users' access to databases to only the access needed to perform their jobs; (2) secure the system it uses to support and manage its computer access request, approval, and review processes; (3) update database

²⁵ See Appendix IV, Number 12.

²⁶ See Appendix IV, Number 13.

²⁷ See Appendix IV, Number 22.

²⁸ Pub. L. No. 104-208, 110 Stat. 3009.

²⁹ See Appendix IV, Number 10.



*Annual Assessment of the Internal Revenue Service
Information Technology Program*

software residing on servers that support its general ledger system; and (4) enable certain auditing features on databases supporting several key systems. In addition, 65 (about 74 percent) of 88 previously reported weaknesses remain unresolved or unmitigated.

The Government Accountability Office stated that until the IRS corrects the identified weaknesses, its financial systems and information remain unnecessarily vulnerable to insider threats, including errors or mistakes and fraudulent or malevolent acts by insiders. As a result, financial and taxpayer information are at increased risk of unauthorized disclosure, modification, or destruction; financial data is at increased risk of errors that result in misstatement; and the IRS's management decisions may be based on unreliable or inaccurate financial information. These weaknesses, considered collectively, were the basis for the Government Accountability Office's determination that the IRS had a material weakness in internal control over financial reporting related to information security in FY 2010.

Continued Emphasis and Attention Is Needed to Allow the Internal Revenue Service to Become a Security-Conscious Organization

As mandated by the Federal Information Security Management Act, we report annually on the effectiveness of the IRS information security program. The Office of Management and Budget identified 10 information security areas to be evaluated under the Federal Information Security Management Act review. Based on our work during the reporting period July 2009 to June 2010, we determined the IRS Information Security Program was generally compliant with Federal Information Security Management Act legislation, Office of Management and Budget requirements, and related information security standards. Specifically, the IRS met the level of performance for three program areas: certification and accreditation, incident response and reporting, and remote access management. While the IRS was generally compliant with the Federal Information Security Management Act legislation, the program was not fully effective as a result of conditions identified in the other seven program areas: configuration management, security training, the process for managing weaknesses, identity and access management, continuous monitoring, contingency planning, and contractor systems/financial audit.

In addition, we identified some security weakness commonalities across several audits during our reporting period.

- The IRS did not follow security evaluative processes prior to deploying systems and technologies.
 - During our review to determine whether General Support Systems security controls have been effectively implemented to ensure Federal tax data are protected, we found the IRS did not conduct adequate risk assessments prior to



*Annual Assessment of the Internal Revenue Service
Information Technology Program*

approving exceptions to required security controls on two General Support Systems.³⁰

- During our review to determine whether the IRS adequately tested and secured the IRS2GO smartphone application that allows taxpayers to check the status of their refunds, we found the IRS2GO application was made available to the public prior to receiving authorization for release. Specifically, the security accreditation and privacy impact assessment was approved after the January 21, 2011, release.³¹
- During our review to determine whether the IRS's current plans for increasing authorized use of wireless technology at IRS facilities are in accordance with Federal wireless security standards, we found that the wireless remote configuration in use at the IRS had not been properly assessed or approved for use in the IRS.³²
- The IRS did not always ensure security controls were implemented on its systems or computer environment.
 - During our review to determine whether the IRS adequately configured databases operating in its nonmainframe environment to properly secure taxpayer data, we identified high- and medium-risk security vulnerabilities on all 13 databases reviewed. These vulnerabilities pertained to account management controls (e.g., default accounts, weak password settings), access privilege management controls (e.g., powerful administrative privileges not assigned based on job functions), and operating system protection controls (e.g., user access to source code).³³
 - During our review to evaluate whether the IRS implemented access controls on its Automated Insolvency System application, we found employees had excessive access privileges to the Automated Insolvency System application because duties were not adequately separated among employees to prevent and detect unauthorized activities and a role-based access control scheme was not adequately implemented on the system.³⁴
 - During our review to determine whether IRS controls, policies, and procedures for sensitive email messages to taxpayers adequately protected taxpayer data, we found the IRS had not implemented an automated control to detect and prevent sensitive tax data in unencrypted emails from being transmitted to those outside the IRS. Prior to November 2007, the IRS maintained a long-standing policy that

³⁰ See Appendix IV, Number 11.

³¹ See Appendix IV, Number 23.

³² See Appendix IV, Number 19.

³³ See Appendix IV, Number 17.

³⁴ See Appendix IV, Number 18.



Annual Assessment of the Internal Revenue Service Information Technology Program

prohibited sending taxpayer data in emails to taxpayers or taxpayers' representatives. The IRS relaxed its email policy in November 2007 when it approved the use of technology to encrypt emails to taxpayers, thereby protecting taxpayer data being sent to and received by taxpayers.³⁵

Until the IRS continues to blend security into its business operations and processes, addresses each computer security material weakness component with the necessary resources and funding, and minimizes the existences of new security weaknesses, the IRS will continue to put the confidentiality, integrity, and availability of financial and taxpayer information maintained and processed on its computer systems at risk.

Information Technology Operations Background

The Enterprise Operations' mission supports the MITS organization by providing efficient, cost-effective, secure, and highly reliable computing (mainframe and server) services for all IRS business entities and taxpayers. The Enterprise Operations organization's Enterprise Computing Center is responsible for providing support for the systems used to receive and process tax returns and payments and all infrastructure servers enterprise-wide and application servers located in the 10 campuses and non-Enterprise Computing Center sites.

The Information Technology Operations Program Has Improved Its Efficiency and Effectiveness

The Information Technology Infrastructure Library[®] is a set of concepts and practices for information technology service management. The Information Technology Infrastructure Library focuses on the key service management principles pertaining to service strategy, service design, service transition, service operation, and continual service improvement.

In September 2010, the Chief Technology Officer outlined a goal to have the MITS organization implement the Information Technology Infrastructure Library best practices over the next several years. The MITS Process Re-Engineering Executive Steering Committee governs the implementation of the Information Technology Infrastructure Library. Responsibility for implementing key Information Technology Infrastructure Library concepts has been assigned to Enterprise Operations executives, with an implementation plan due in September 2011.

In addition, the Quality Assurance Program Office is part of the Applications Development function's effort in leading a MITS organization-wide initiative to use the Software Engineering Institute's Capability Maturity Model Integration. The Capability Maturity Model Integration consists of best practices that organizations follow to improve effectiveness, efficiency, and quality of their product and service development work. Specifically, the MITS organization is

³⁵ See Appendix IV, Number 16.



Annual Assessment of the Internal Revenue Service Information Technology Program

planning to use the Capability Maturity Model Integration-Development model to help improve its development and maintenance processes for both products and services.

During FY 2011, we conducted several audits on information technology operations and found the IRS is taking steps to improve operational efficiency and effectiveness.

- During our review to evaluate the efficiency and effectiveness of the capacity and performance management of the IRS mainframe computing environment, we found the capacity management policy and procedures have incorporated Information Technology Infrastructure Library best practice principles. We also found personnel responsible for the capacity management of the IBM and Unisys mainframe environments are actively monitoring mainframe performance against their own informal measures. The IBM capacity managers create an annual capacity report, as well as various day-to-day application-specific reports. The Unisys capacity managers create periodic reports on daily, weekly, and weekend transaction processing.³⁶
- During our review to determine whether the Service Operations Command Center Branch has effectively implemented Information Technology Infrastructure Library best practices, we found the Service Operations Command Center Branch has incorporated the Information Technology Infrastructure Library best practice principles of Event Management, Incident Management, and Problem Management into its Concept of Operations and policies and procedures. In addition, the Service Operations Command Center Branch has made these best practices a part of the way it does business by utilizing a Knowledge Database. Lastly, our review of Priority 1 and Priority 2 incident tickets determined tickets worked by Command Center personnel were resolved within documented service level agreement time periods.³⁷
- During our review to determine whether the Applications Development function's Quality Assurance Program Office ensures development projects implement a coordinated set of activities that conform to organizational policies, processes, and procedures that meet the standards of the Software Engineering Institute's Capability Maturity Model Integration – Development maturity level 2, we found the Quality Assurance Program Office's processes, guidance, and procedures generally meet the Capability Maturity Model Integration maturity level 2 requirements for quality assurance.³⁸
- During our review to determine the effectiveness of the IRS efforts to address the critical issue of sustaining the IRS information technology infrastructure, we found the Sustaining Infrastructure Program developed and implemented a process for identifying,

³⁶ See Appendix IV, Number 27.

³⁷ See Appendix IV, Number 24.

³⁸ See Appendix IV, Number 5.



Annual Assessment of the Internal Revenue Service Information Technology Program

reviewing, prioritizing, and making decisions on funding the replacement of aged computer hardware as well as other critical infrastructure needs. The Sustaining Infrastructure Program is significantly improved, and agreed-upon prior recommendations are being implemented. The annual baseline amount allocated to the Sustaining Infrastructure Program is approximately \$150 million, and the program is centralized to ensure the replacement of the IRS information technology infrastructure is addressed corporately.³⁹

As a result of implementing the best practices and consolidating security activities, the IRS reported \$75 million in operational efficiencies gained in its FY 2012 budget request justification. While operational efficiencies have been reported, additional opportunities to improve operations remain.

Actions have been taken to improve the energy efficiency of desktop computer equipment

On January 24, 2007, President George W. Bush signed Executive Order 13423, *Strengthening Federal Environmental, Energy, and Transportation Management*. The purpose of this policy was to strengthen the environmental, energy, and transportation management of Federal agencies by “conducting their environmental, transportation, and energy-related activities under the law in support of their respective missions in an environmentally, economically, and fiscally sound, integrated, continuously improving, efficient, and sustainable manner.” In July 2007, the Department of the Treasury established the Electronics Stewardship Program and Implementation Plan to ensure sustainable practices in the area of electronics and to provide policy and guidance regarding acquisition, operations and maintenance, and end-of-life management.

Executive Order 13423 requires Federal agencies to, in part:

- Improve energy efficiency of agency facilities 3 percent annually through the end of FY 2015 or 30 percent by FY 2015 compared to the FY 2003 baseline year, thereby reducing greenhouse gas.
- Acquire electronic products (at least 95 percent) that are an Electronic Product Environmental Assessment Tool-registered product, unless there is no Electronic Product Environmental Assessment Tool standard for such product, and enable ENERGY STAR[®] features on agency computers and monitors.

The Electronic Product Environment Assessment Tool is a system that helps purchasers evaluate, compare, and select electronic products based on their environmental attributes. ENERGY STAR is a joint program of the Environmental Protection Agency and the Department of Energy

³⁹ See Appendix IV, Number 21.



Annual Assessment of the Internal Revenue Service Information Technology Program

designed to help save money and protect the environment through energy efficient products and practices.

During our review to determine whether the IRS has taken effective steps to ensure the acquisition, operation, and maintenance of energy efficient desktop computer equipment, we determined the IRS is purchasing energy efficient desktop computer equipment and has enabled an energy saving feature on computer monitors that puts the monitors in “sleep mode” during periods of inactivity.⁴⁰

Operational efficiency and effectiveness can be improved

The Clinger-Cohen Act of 1996⁴¹ requires agencies to use a disciplined capital planning and investment control process to maximize the value of information technology investments and manage the acquisition risk.

During FY 2011, we conducted several audits on information technology operations and found opportunities for the IRS to improve operational efficiency and effectiveness.

- During our review to evaluate the efficiency and effectiveness of the capacity and performance management of the IRS mainframe environment, we found license costs for the software products residing on the IRS mainframes are tied to the mainframe capacity, or number of Millions of Instructions Per Second (allocated to the machines). A whitepaper prepared by the IRS noted that there is an opportunity for the IRS to reduce its software license costs by changing the measure it uses to calculate the capacity of its mainframes from Millions of Instructions Per Second to Millions of Service Units. Had the IRS made the conversion from a Millions of Instructions Per Second basis for determining the capacity of its IBM mainframes to Millions of Service Units, the IRS could have realized software licensing cost savings of \$580,358, using the 10 percent reduction estimate in the IRS whitepaper.⁴²
- During our review to determine whether the Service Operations Command Center Branch has effectively implemented Information Technology Infrastructure Library best practices, we found Command Center personnel should examine incident reports to identify trends within the information technology infrastructure, Command Center Branch management needs to conduct a baseline assessment of its staffing and workload, the Service Operations Command Center Branch needs to have a documented strategic plan to communicate its goals and priorities with milestone and target dates, and

⁴⁰ See Appendix IV, Number 20.

⁴¹

⁴² See Appendix IV, Number 27.



*Annual Assessment of the Internal Revenue Service
Information Technology Program*

personnel need customized training to effectively implement the Information Technology Infrastructure Library.⁴³

- During our review to determine whether adequate security controls have been established for the IBM DB2 databases running on the IBM z/OS operating system, we found the security policies and configuration settings were in compliance with Government and industry standards and effectively implemented.

However, in July 2010, the Cybersecurity organization purchased the IBM Guardium software application to perform automated vulnerability scans of its databases. The enterprise-wide software license covering 3,000 processors and the hardware needed to perform automated vulnerability scans cost \$3.3 million. The IRS originally anticipated implementation by December 2010. However, by July 2011, the IBM Guardium software application still had not been implemented enterprise-wide because of, according to IRS management, other higher priorities and the lack of support needed from several organizations. In June 2011, the IRS received an invoice for approximately \$700,000 to renew the annual software application license. This invoice was paid in order to continue deployment and avoid penalties for a lapse in maintenance; however, the application had not been fully implemented, resulting in an inefficient use of resources.⁴⁴

- During our review to determine whether the Applications Development function's Quality Assurance Program Office ensures development projects implement a coordinated set of activities that conform to organizational policies, processes, and procedures that meet the standards of the Software Engineering Institute's Capability Maturity Model Integration – Development maturity level 2, we found the Quality Assurance Program Office audit documentation and procedures need improvement.⁴⁵
- During our review to determine whether the IRS has taken effective steps to ensure the acquisition, operation, and maintenance of energy efficient desktop computer equipment, we determined the IRS has not established an implementation strategy to ensure timely completion of applicable action items in the Electronics Stewardship Program and Implementation Plan. For example, timely actions have not been taken to implement power management (e.g., power down/sleep mode) functionality on desktop computers (also includes laptop computers). Policies and procedures have not been established to implement duplex (two-sided) printing on printers.⁴⁶

⁴³ See Appendix IV, Number 24.

⁴⁴ See Appendix IV, Number 26.

⁴⁵ See Appendix IV, Number 5.

⁴⁶ See Appendix IV, Number 20.



*Annual Assessment of the Internal Revenue Service
Information Technology Program*

Measuring and reporting operational results can be improved

Industry best practices emphasize that identifying the appropriate measures, creating a process for collecting and analyzing the data, and effectively using the data to guide and direct continued improvement are essential to establishing a successful measurement process. Meaningful key performance indicators should align with organizational goals and provide insight into the following: Quality, Efficiency, Compliance, and Value. Also, metrics should be specific, measurable, attainable, realistic, and time driven. Metrics help to ensure that the process in question is running effectively and efficiently.

During FY 2011, two audits we conducted identified opportunities to improve the measuring and reporting operational results.

- During our review to evaluate the efficiency and effectiveness of the capacity and performance management of the IRS mainframe environment, we found performance measurement requirements in Defined-Service Agreements are not formally established to facilitate the management and reporting of mainframe performance. Our review of the 20 Defined-Service Agreements found that the Enterprise Operations organization is not consistently including measurable performance metrics such as availability, reliability, performance, and capacity in these agreements. Only 4 of the 20 Defined-Service Agreements contained any measurable performance metrics.⁴⁷
- During our review to determine whether the Service Operations Command Center Branch has effectively implemented Information Technology Infrastructure Library best practices, we found additional measures are needed to capture the improved efficiency and effectiveness resulting from the Information Technology Infrastructure Library.⁴⁸

⁴⁷ See Appendix IV, Number 27.

⁴⁸ See Appendix IV, Number 24.



*Annual Assessment of the Internal Revenue Service
Information Technology Program*

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to assess the status of the IRS's Information Technology Program since June 2010 as required by the IRS Restructuring and Reform Act of 1998.¹ The scope of this assessment covers information technology security, modernization, and operations and includes the TIGTA audit reports that have been issued to the IRS from June 2010 through July 2011.

- I. Determined and provided an overall assessment of the IRS's Information Technology Program.
 - A. Assessed the **Information Technology Security and Privacy** issues. We determined which are at high risk for delivering IRS program objectives and protecting tax administration data by analyzing the TIGTA Security Directorate audit report issues identified during the period June 2010 through July 2011. We also reviewed the prior three annual assessment reports for any trends in security and privacy issues.
 - B. Assessed **Information Technology Modernization** issues. We determined which are at high risk for delivering IRS program objectives and protecting tax administration data by analyzing the TIGTA Modernization Directorate audit report issues identified during the period June 2010 through July 2011. We also reviewed the prior three annual assessment reports for any trends in modernization issues.
 - C. Assessed **Information Technology Operations** issues. We determined which are at high risk for delivering IRS program objectives and protecting tax administration data by analyzing the TIGTA Operations Directorate audit report issues identified during the period June 2010 through July 2011. Operations issues were not included in the prior annual assessment reports.
 - D. Reviewed the TIGTA open audit inventory to identify ongoing audits of Information Technology security, modernization, and operations. We contacted audit staff to identify and clarify issues and obtain current estimates of report due dates.
 - E. Met with each audit director and the Assistant Inspector General for Audit to discuss high-level messages or themes they determined are relevant and important to be conveyed through this year's annual assessment report.

¹ Pub. L. No. 105-206, 112 Stat. 685 (codified as amended in scattered sections of 2 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.).



*Annual Assessment of the Internal Revenue Service
Information Technology Program*

- F. Discussed with the applicable audit directors and Assistant Inspector General for Audit whether the IRS's current information technology security and modernization material weaknesses² should remain or be downgraded.
- G. Reviewed and summarized any relevant congressional testimony and high-level briefings the TIGTA presented pertaining to IRS's information technology security, modernization, and operations.
- H. Reviewed the April 2011 Interim Filing Season Report.
- II. Determined and summarized the results of any applicable oversight assessments of the IRS's information technology security, modernization, and operations.
 - A. Obtained, reviewed, and summarized applicable studies, reports, and legislative guidance from congressional committees.
 - B. Obtained, reviewed, and summarized applicable studies, reports, and guidance from the IRS Oversight Board.
 - C. Obtained, reviewed, and summarized relevant Government Accountability Office reports.
 - D. Summarized the results of any IRS assessments and status information pertaining to the IRS's Information Technology security, modernization, and operations. We reviewed key documents such as the Chief Technology Officer's position on information technology material weaknesses, the IRS's Modernization Vision and Strategy Program, MITS Business Value Chart, the IRS's Information Technology Security Program Plan, the Business Systems Modernization Expenditure Plan, and the Fiscal Year 2012 IRS budget request justification.

Internal controls methodology

Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We did not evaluate internal controls as part of this review because doing so was not necessary to satisfy our review objective.

² See Appendix VI for a glossary of terms.



*Annual Assessment of the Internal Revenue Service
Information Technology Program*

Appendix II

Major Contributors to This Report

Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
Diana M. Tengesdal, Acting Director
Danny Verneuille, Director
Kimberly R. Parmley, Audit Manager
Charlene L. Elliston, Lead Auditor
Cari D. Fogle, Senior Auditor
Mary L. Jankowski, Senior Auditor
Ryan M. Perry, Senior Auditor
Hung Q. Dam, Information Technology Specialist
Kevin Liu, Information Technology Specialist



*Annual Assessment of the Internal Revenue Service
Information Technology Program*

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Chief, Agency-Wide Shared Services OS:A
Deputy Commissioner of Operations SE:W
Deputy Chief Information Officer for Strategy/Modernization OS:CTO
Associate Chief Information Officer, Affordable Care Act (PMO) OS:CTO:ACA
Associate Chief Information Officer, Applications Development OS:CTO:AD
Associate Chief Information Officer, Cybersecurity OS:CTO:C
Associate Chief Information Officer, Enterprise Operations OS:CTO:EO
Associate Chief Information Officer, Enterprise Network OS:CTO:EN
Associate Chief Information Officer, Enterprise Services OS:CTO:ES
Associate Chief Information Officer, Modernization Program Management Office OS:CTO:MP
Associate Chief Information Officer, Strategy and Planning OS:CTO:SP
Director, Procurement OS:A:P
Director, Compliance OS:CTO:C
Director, CADE 2 Database Implementation OC:CTO:AD
Director, Program Management OS:CTO:AD:PM
Director, Privacy, Information Protection and Data Security OS:P
Director, Privacy, and Information Protection OS:PIP
Director, Cybersecurity Operation OS:CTO:C
Director, CADE 2/Health Care ACA OS:CTO:EO
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 Internal Control OS:CFO:CPIC:IC
Audit Liaisons:
 Associate Chief Information Officer, Applications Development OS:CTO:AD
 Director, Risk Management Division OS:CTO:SP:RM



*Annual Assessment of the Internal Revenue Service
Information Technology Program*

Appendix IV

*Listing of Treasury Inspector General for Tax
Administration Reports Reviewed*

Number	Report Reference or (Audit) Number	Report Title	Report Issuance Date
1	2010-20-099	The Federal Student Aid Datashare Application Was Successfully Deployed, but Improvements in Systems Development Disciplines Are Needed	Final Report Issued September 2010
2	2010-21-110	The Internal Revenue Service Should Strengthen Processes for Managing Recovery Act Funds Used for the Health Coverage Tax Credit	Final Report Issued September 2010
3	2010-20-094	Annual Assessment of the Business Systems Modernization Program	Final Report Issued September 2010
4	2011-20-001	Prototype Process Improvements Will Benefit Efforts to Modernize Taxpayer Account Administration	Final Report Issued November 2010
5	2011-20-007	The Applications Development Function's Quality Assurance Program Office Can Make Its Processes More Effective	Final Report Issued February 2011
6	2011-20-088	The Modernized e-File Release 6.2 Included Enhancements, but Improvements Are Needed for Tracking Performance Issues and Security Weaknesses	Final Report Issued September 2011
7	(201120001)	The Customer Account Data Engine 2 Is Making Progress Toward Achieving Daily Processing, but Improvements Are Warranted to Ensure Full Functionality	Draft Report Issued August 2011
8	2011-20-110	The Customer Account Data Engine 2 Database Implementation Project Made Progress in Design Activities, but Improvements Are Needed	Final Report Issued September 2011



*Annual Assessment of the Internal Revenue Service
Information Technology Program*

Number	Report Reference or (Audit) Number	Report Title	Report Issuance Date
9	(201020025)	The Customer Account Data Engine 2 Program Management Office Implemented Systems Development Guidelines; However, Process Improvements Are Needed to Address Inconsistencies	Draft Report Issued August 2011
10	2010-10-065	Measurable Progress Has Been Made in Addressing Federal Financial Management Improvement Act Noncompliance; However, Significant Challenges Remain	Final Report Issued June 2010
11	2010-20-063	Sensitive But Unclassified – Implementation of General Support Systems Security Controls Needs Improvement to Protect Taxpayer Data	Final Report Issued June 2010
12	2010-20-082	Sensitive But Unclassified – Additional Actions and Resources Are Needed to Resolve the Audit Trail Portion of the Computer Security Material Weakness	Final Report Issued July 2010
13	2010-20-084	More Actions Are Needed to Correct the Security Roles and Responsibilities Portion of the Computer Security Material Weakness	Final Report Issued August 2010
14	2010-20-101	Treasury Inspector General for Tax Administration – Federal Information Security Management Act (Non-Intelligence National Security Systems) Report for Fiscal Year 2010	Final Report Issued September 2010
15	2011-20-003	Treasury Inspector General for Tax Administration – Federal Information Security Management Act Report for Fiscal Year 2010	Final Report Issued November 2010
16	2011-20-012	Additional Security Is Needed for the Taxpayer Secure Email Program	Final Report Issued February 2011
17	2011-20-044	Security Over Databases Could Be Enhanced to Ensure Taxpayer Data Are Protected	Final Report Issued May 2011
18	2011-20-046	Access Controls for the Automated Insolvency System Need Improvement	Final Report Issued May 2011



*Annual Assessment of the Internal Revenue Service
Information Technology Program*

Number	Report Reference or (Audit) Number	Report Title	Report Issuance Date
19	2011-20-101	Security Controls Over Wireless Technology Were Generally in Place; However, Further Actions Can Improve Security	Final Report Issued September 2011
20	2010-20-056	Additional Efforts Are Needed to Implement the Electronics Stewardship Program and Maximize the Energy Efficiency of Desktop Computer Equipment	Final Report Issued June 2010
21	2011-20-006	The Sustaining Infrastructure Program Is Significantly Improved and a Comprehensive Information Technology Infrastructure Strategy Has Been Developed	Final Report Issued December 2010
22	2011-20-060	Corrective Actions to Address the Disaster Recovery Material Weakness Are Being Completed	Final Report Issued June 2011
23	2011-20-076	The IRS2GO Smartphone Application Is Secure, but Development Process Improvements Are Needed	Final Report Issued August 2011
24	2011-20-078	Service Operations Command Center Management Can Do More to Benefit From Implementing the Information Technology Infrastructure Library	Final Report Issued August 2011
25	2011-20-105	The Modernization and Information Technology Services Organization Is Effectively Planning for the Implementation of the Affordable Care Act	Final Report Issued September 2011
26	(201120021)	The Mainframe Databases Reviewed Met Security Requirements; However, Automated Security Scans Were Not Performed	Draft Report Issued August 2011
27	2011-20-074	Mainframe Computer Performance Is Being Actively Monitored, but Defined-Service Agreements and Software Licensing Can Be Improved	Final Report Issued September 2011
28	(201140030)	Low Participation and Tax Return Volumes Continue to Hinder the Transition of Individual Income Tax Returns to the Modernized e-File System	Draft Report Issued August 2011



*Annual Assessment of the Internal Revenue Service
Information Technology Program*

Appendix V

Project Cost and Schedule Variances

This table presents the cost and schedule variance for the Modernization Program project releases¹ delivered in FY 2011 through June 2011.

Release	Current Finish Date	Milestone	Current Cost (000)	Cost Variance (Percentage)	Schedule Variance (Days)	Schedule Variance (Percentage)
Current CADE						
6.2	January 14, 2011	4b	22,000	0%	-10 ²	-6%
CADE 2						
Trans State 1	April 18, 2011	3-4a	24,200	0%	-11	-6%
MeF						
6.2	May 18, 2011	4b-5	13,000	0%	1	1%
7	April 26, 2011	3-4a	27,705	-24% ³	0	0%

Source: *Business Systems Modernization Monthly Performance Measures Report, issued July 5, 2011.*

¹ See Appendix VI for a glossary of terms.

² A negative schedule variance indicates the milestone was completed before the planned date.

³ According to the IRS, this variance resulted from lower than expected hardware and software costs.



*Annual Assessment of the Internal Revenue Service
Information Technology Program*

Appendix VI

Glossary of Terms

Term	Definition
Account Management Services	The Account Management Services project will modernize the capability to collect, view, retrieve, and manage taxpayer information.
Best Practice	A technique or methodology that, through experience and research, has proven to reliably lead to a desired result.
Business Systems Modernization	The Business Systems Modernization Program, which began in 1999, is a complex effort to modernize the IRS's technology and related business processes.
Capability Maturity Model [®]	A structured process that helps organizations improve their abilities to consistently and predictably acquire and develop high-quality information systems. Organizations that have implemented Capability Maturity Model processes have seen dramatic improvements in their abilities to meet planned time periods, reduce errors, and increase value on dollars invested.
Customer Account Data Engine (CADE)	The foundation for managing taxpayer accounts in the IRS modernization plan. It will consist of databases and related applications that will replace the existing IRS Master File processing systems and will include applications for daily posting, settlement, maintenance, refund processing, and issue detection for taxpayer tax account and return data.
Customer Account Data Engine 2 (CADE 2)	Creates a modernized processing and data-centric infrastructure that will enable the IRS to improve the accuracy and speed of individual taxpayer account processing, enhance the customer experience through improved access to account information, and increase the effectiveness and efficiency of agency operations.
Enterprise Life Cycle	A structured business systems development method that requires the preparation of specific work products during different phases of the development process.



*Annual Assessment of the Internal Revenue Service
Information Technology Program*

Term	Definition
Federal Information Security Management Act of 2002	Legislation which requires the Inspector General to perform an annual independent evaluation of each Federal agency's information security policies, procedures, and practices as well as evaluate its compliance with this law.
Filing Season	The period from January through mid-April when most individual income tax returns are filed.
Fiscal Year	A 12-consecutive-month period ending on the last day of any month except December. The Federal Government's fiscal year begins on October 1 and ends on September 30.
Master File	The IRS database that stores various types of taxpayer account information. This database includes individual, business, and employee plans and exempt organizations data.
Material Weakness	Office of Management and Budget Circular A-123, <i>Management's Responsibility for Internal Control</i> , dated December 2004, defines a material weakness as any condition an agency head determines to be significant enough to be reported outside the agency.
Milestone	The "go/no-go" decision point in a project; it is sometimes associated with funding approval to proceed.
Modernized e-File	The Modernized e-File project develops the modernized, web-based platform for filing approximately 330 IRS forms electronically, beginning with the U.S. Corporation Income Tax Return (Form 1120), U.S. Income Tax Return for an S Corporation (Form 1120S), and Return of Organization Exempt From Income Tax (Form 990). The project serves to streamline filing processes and reduce the costs associated with a paper-based process.
Plan of Action and Milestones	A requirement for managing the security weaknesses pertaining to a specific application or system. In addition to noting weaknesses, each Plan of Action and Milestones item details steps that need to be taken to correct or reduce any weaknesses, as well as resources required to accomplish task milestones and a correction timeline.
Release	A specific edition of software.



*Annual Assessment of the Internal Revenue Service
Information Technology Program*

Term	Definition
Software Engineering Institute	A federally funded research and development center operated by Carnegie Mellon University and sponsored by the Department of Defense. Its objective is to provide leadership in software engineering and in the transition of new software engineering technology into practice.