



*Modernized e-File Will Enhance Processing of
Electronically Filed Individual Tax Returns,
but System Development and Security
Need Improvement*

May 26, 2010

Reference Number: 2010-20-041

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.



HIGHLIGHTS

MODERNIZED E-FILE WILL ENHANCE PROCESSING OF ELECTRONICALLY FILED INDIVIDUAL TAX RETURNS, BUT SYSTEM DEVELOPMENT AND SECURITY NEED IMPROVEMENT

Highlights

Final Report issued on May 26, 2010

Highlights of Report Number: 2010-20-041 to the Internal Revenue Service Chief Technology Officer.

IMPACT ON TAXPAYERS

The Modernized e-File Project's (MeF) goal is to replace the Internal Revenue Service's (IRS) current tax return filing technology with a modernized, Internet-based electronic filing platform. This will allow more individual taxpayers to take advantage of the benefits of electronic filing, while streamlining the IRS' filing processes and reducing the costs associated with paper tax returns. The IRS' management of the Project's risks, requirements, and security can be improved to ensure the capabilities expected and approved to be deployed are appropriately implemented.

WHY TIGTA DID THE AUDIT

This review was part of our Fiscal Year 2010 Annual Audit Plan and addresses the major management challenge of Modernization of the IRS. The overall objective of this review was to determine whether the MeF Project Release 6.1 development activities provided the capability to electronically receive, process, and secure U.S. Individual Income Tax Returns (Form 1040), delivering the intended benefits to the IRS and taxpayers.

WHAT TIGTA FOUND

On February 17, 2010, the IRS deployed MeF Release 6.1 and began processing electronically filed individual income tax forms. During the first 3 weeks of operation, the MeF system rejected 23 percent of the individual income tax returns filed.

The System Integration Test Results indicated all application requirements were tested and passed. However, supporting test documents showed that many of the requirements were not tested and many more failed the tests and no indication was provided to show the defects were corrected. Additionally, reviewing prior release development and deployment experiences – Lessons Learned Reports – would improve project management.

Further, controls were not adequate to manage all of the MeF system security risks, issues, and action items. Information provided by the IRS in December 2009, showed that 10 of the 13 security vulnerabilities were resolved. However, the January 2010 Security Test and Evaluation reported that only 2 of the 13 vulnerabilities were resolved.

WHAT TIGTA RECOMMENDED

TIGTA recommended the Chief Technology Officer ensure that project releases are deployed only after all system requirements are tested and met and that test results are verified to ensure their completeness and accuracy. Further, guidance should be modified to require consideration of Lessons Learned Reports earlier in the project development process.

To resolve all MeF system security issues, the Cybersecurity organization must complete implementation of the process to ensure that system owners enter and track all system security weaknesses in IRS control systems.

In its response to the report, the IRS stated it plans to update project development guidance and that it completed the process to control system security weaknesses as of March 25, 2010. The IRS disagreed with the recommendation about release deployment only after testing showed requirements were met, citing milestone readiness reviews and the Executive Steering Committee as controls. With the significant number of failed tests and the resulting problems in rejected individual income tax returns filed, TIGTA questions whether the Executive Steering Committee had sufficient and timely information to make an informed risk-based decision for deploying MeF Release 6.1.



TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

May 26, 2010

MEMORANDUM FOR CHIEF TECHNOLOGY OFFICER

FROM: (for) Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Modernized e-File Will Enhance Processing of Electronically Filed Individual Tax Returns, but System Development and Security Need Improvement (Audit # 200920023)

This report presents the results of our review of the Modernized e-File Project Release¹ 6.1 development activities. The overall objective of this review was to determine whether the Modernized e-File Project Release 6.1 development activities will provide the capability to electronically receive, process, and secure U.S. Individual Income Tax Returns (Form 1040), delivering the intended benefits to the Internal Revenue Service and taxpayers. This review was part of our Fiscal Year 2010 Annual Audit Plan and addresses the major management challenge of Modernization of the Internal Revenue Service.

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

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

¹ See Appendix VI for a glossary of terms.



*Modernized e-File Will Enhance Processing of
Electronically Filed Individual Tax Returns, but
System Development and Security Need Improvement*

Table of Contents

Background	Page 1
Results of Review	Page 3
The Modernized e-File Project Adds New Electronic Filing Capabilities and Improves Existing Capabilities	Page 3
The Modernized e-File Project Team Has Not Completely Addressed Previously Reported Requirements Management and Processing Issues.....	Page 4
<u>Recommendation 1</u> :.....	Page 6
The Modernized e-File Project Team Generally Followed Established Systems Development Processes, but Can Improve Its Management of Requirements and Risks.....	Page 7
<u>Recommendations 2 and 3</u> :	Page 11
Modernized e-File Security Issues Were Not Adequately Controlled or Resolved	Page 12
<u>Recommendation 4</u> :.....	Page 17
Appendices	
Appendix I – Detailed Objective, Scope, and Methodology	Page 18
Appendix II – Major Contributors to This Report.....	Page 22
Appendix III – Report Distribution List	Page 23
Appendix IV – Enterprise Life Cycle Overview	Page 24
Appendix V – Status of Resolution for Modernized e-File System Security Vulnerabilities and Security Findings	Page 26
Appendix VI – Glossary of Terms.....	Page 31
Appendix VII – Management’s Response to the Draft Report.....	Page 34



*Modernized e-File Will Enhance Processing of
Electronically Filed Individual Tax Returns, but
System Development and Security Need Improvement*

Abbreviations

IRS	Internal Revenue Service
MeF	Modernized e-File
MITS	Modernization and Information Technology Services
TIGTA	Treasury Inspector General for Tax Administration



*Modernized e-File Will Enhance Processing of
Electronically Filed Individual Tax Returns, but
System Development and Security Need Improvement*

Background

The Modernized e-File (MeF) system is a replacement of the current Internal Revenue Service (IRS) tax return filing technology with a modernized, Internet-based electronic filing platform. This system streamlines tax return filing processes and reduces the costs associated with paper tax returns.

The MeF system supports and facilitates the IRS' commitment to achieve the IRS Restructuring and Reform Act of 1998 goal of receiving at least 80 percent of all tax returns in electronic form.

In February 2004, the IRS deployed the initial MeF system release.¹ This release provided Internet-based filing of the U.S. Corporation Income Tax Return (Form 1120), the U.S. Income Tax Return for an S Corporation (Form 1120S), and the Return of Organization Exempt From Income Tax (Form 990). The MeF Project also developed the Federal/State Single Point Filing System platform and the Federal/State components for Forms 1120 and 990, permitting tax return transmitters to submit multiple Federal and State tax return types within one electronic transmission.

Subsequent releases added the U.S. Return of Partnership Income (Form 1065), U.S. Return of Income for Electing Large Partnerships (and Form 1065-B), excise tax forms associated with the Excise Tax *e-File* and Compliance project, U.S. Income Tax Return of a Foreign Corporation (Form 1120-F), and the Electronic Notice (e-Postcard) for Tax-Exempt Organizations Not Required to File Form 990 or 990-EZ (Form 990-N).

MeF Release 6.1 was deployed in February 2010 and includes 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 Form 1040 for Tax Year 2009. Future releases will include hardware installation for full Form 1040 implementation, full disaster recovery capability, and the remaining Form 1040 related forms (approximately 120 forms).

For all forms submitted, electronic filing transmitters use IRS approved software to allow them to electronically file tax returns. Returns received electronically are validated for format and content, and an acknowledgement is returned to the transmitter indicating whether the return was accepted or rejected. Accepted returns are stored in the Modernized Tax Return Database, the legal repository for original electronically filed tax returns received by the IRS through the MeF system, and forwarded to IRS downstream systems for further tax processing.

The MeF system is 1 of more than 200 computer systems maintained by the IRS to administer the nation's tax system. Each tax return contains personally identifiable information, such as the

¹ See Appendix VI for a glossary of terms.



*Modernized e-File Will Enhance Processing of
Electronically Filed Individual Tax Returns, but
System Development and Security Need Improvement*

filer's name, address, Social Security Number, and other personal information. Because of the volume and type of data it maintains, the IRS is an attractive target for criminals with the intent to commit identity theft by stealing and using someone's personal information for their own financial gain.

Like all Federal Government agencies, the IRS should protect its computer systems by implementing appropriate security controls to ensure the confidentiality, integrity, and availability of sensitive data, as recommended in the National Institute of Standards and Technology Special Publication 800-53.² These security controls include system access, audit logging, and contingency planning. In addition, the IRS is specifically required by Federal law³ to keep taxpayer data confidential and prevent unauthorized disclosure or browsing of taxpayer records. These requirements apply to all IRS computer systems that maintain sensitive data.

The IRS stores sensitive financial and personal information for more than 130 million individual taxpayers who file annual Federal income tax returns.

This review was performed at the Modernization and Information Technology Services (MITS) organization facilities in New Carrollton, Maryland, during the period August 2009 through February 2010. We conducted this performance audit 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 objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. This review was included in the Treasury Inspector General for Tax Administration (TIGTA) Fiscal Year 2010 Annual Audit Plan and addresses the major management challenge of Modernization of the IRS. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

² *Recommended Security Controls for Federal Information Systems*, Revision 2, dated December 2007.

³ Internal Revenue Code Section 6103 (26 U.S.C. Section 6103) and the Taxpayer Browsing Protection Act of 1997 (26 U.S.C.A. Sections 7213, 7213A, 7431 (West 2006)).



*Modernized e-File Will Enhance Processing of
Electronically Filed Individual Tax Returns, but
System Development and Security Need Improvement*

Results of Review

The Modernized e-File Project Adds New Electronic Filing Capabilities and Improves Existing Capabilities

The IRS deployed Release 6.1 on February 17, 2010, and for the first time, began processing electronically filed individual tax forms on the MeF system. MeF Release 6.1 also permits tax return transmitters to submit multiple Federal and State individual tax returns within one electronic transmission. MeF Release 6.1 provides benefits by improving individual tax return filing and processing efficiency and by being the system that provides tax form information to other IRS systems for use by employees.

The MeF Release 6.1 development included a plan to effectively manage the expected large processing volume of individual tax returns and requests for an extension to file. This plan incorporates a prudent approach by limiting the volume of forms for processing in Calendar Year 2010 so the IRS and tax form transmitters have an opportunity to observe system behavior and responses. Based on the system performance in Calendar Year 2010, the MeF system can be adjusted to manage the full workload of individual tax returns during Calendar Year 2011.

The plan controls the volume of processing by providing participating transmitters a limit to the number of forms they can submit daily. The daily totals are based on 2009 volumes and discussions held with the transmitters. Based on agreements with transmitters, the IRS estimates MeF Release 6.1 will process the following volumes of individual tax forms during the periods specified:

- February 17, 2010, through February 28, 2010 – 1.5 million forms.
- March 1, 2010, through March 31, 2010 – 4.4 million forms.
- April 1, 2010, through April 15, 2010 – 5 million forms.

Based on these estimates, MeF Release 6.1 will process during these periods almost 11 million of the 15.6 million projected total individual tax forms the MeF system is expected to receive electronically.



Modernized e-File Will Enhance Processing of Electronically Filed Individual Tax Returns, but System Development and Security Need Improvement

The Modernized e-File Project Team Has Not Completely Addressed Previously Reported Requirements Management and Processing Issues

Verifying Development of Requirements: In a prior TIGTA audit report entitled *The Modernized e-File Project Can Improve Its Management of Requirements*,⁴ we recommended Project Teams follow the Enterprise Life Cycle⁵ provisions for managing requirements by ensuring planned capabilities were developed by tracing release requirements in the System Requirements Report to the requirements traceability verification matrices. In addition, we recommended the Project Team document implementation of all requirements throughout the project life cycle in the System Requirements Report. The IRS' corrective action for MeF Requirements Traceability indicated that for Release 6, the MeF Project was working with the Business Rules and Requirements Management office to implement a full bi-directional traceability model. The IRS reported implementation of the corrective actions was completed January 16, 2009.

To determine if the MeF Release 6.1 requirements were adequately traced between the high-level and low-level requirements, we reviewed the:

- Business System Requirements Report Final, System Development Phase (Milestone 4b), dated December 3, 2009, which presents all of the requirements for implementation in Release 6.1.
- System Integration and Test Plan, Appendix A – Integration, Test, and Deployment Requirements Traceability Verification Matrix, dated November 3, 2009, which presents the bi-directional traceability between the release requirements and the related test cases.

We selected a sample of customer and system requirements to verify the adequacy of the bi-directional traceability for the MeF Release 6.1 requirements. The project staff performed the bi-directional requirements tracing between the Business System Requirements Report Final and the System Integration and Test Plan as required by the Enterprise Life Cycle.

The System Integration and Test End of Test Completion Report documents actual testing results and identifies applicable environmental, test approach, test design, test planning, and test execution variances from the original Test Plan. The Requirements Traceability Verification Matrix delivered in the original Test Plan must be updated to document the actual results of test execution. On March 5, 2010, after we had held our closing conference with the IRS, the Project Team provided the System Integration and Test End of Test Completion Report, dated January 22, 2010, which reported that all MeF Release 6.1 capabilities passed testing. Subsequently, on March 8, 2010, the Project Team provided Appendix A, which included two

⁴ Reference Number 2007-20-099, dated July 9, 2007.

⁵ See Appendix IV for an overview of the Enterprise Life Cycle.



Modernized e-File Will Enhance Processing of Electronically Filed Individual Tax Returns, but System Development and Security Need Improvement

matrices – the Test, Assurance, and Documentation Requirements Traceability Verification Matrix and the Integration, Test, and Deployment Requirements Traceability Verification Matrix. The test execution results presented for the Test, Assurance, and Documentation Requirements Traceability Verification Matrix reported failed tests and defect reports for the MeF Release 6.1. These failed test results were not accurately summarized in the final report. Additionally, the Integration, Test, and Deployment Requirements Traceability Verification Matrix did not present any test execution results. The following table presents the tests results reported in the System Integration and Test End of Test Completion Report summary and in each of the traceability verification matrix sections.

Table 1: MeF Release 6.1 Testing Results

Section of System Integration and Test End of Test Completion Report	Number of Failed Tests	Number of Test Cases With Defect Reports
Report Summary	0	8
Appendix A – Integration, Test, and Deployment Requirements Traceability Verification Matrix	No Results Provided	No Results Provided
Appendix A – Test, Assurance, and Documentation Requirements Traceability Verification Matrix	34	120

Source: System Integration and Test End of Test Completion Report, dated January 22, 2010.

The Test, Assurance, and Documentation Requirements Traceability Verification Matrix also presented the following results about uncompleted tests: 29 blocked; 37 not run; 4 in progress; and 17 candidates for waiver. None of these results were included in the report body summary, and when asked about these conditions, the IRS did not provide an explanation for the conflicts between the final report and the supporting documentation.

Although the Project Team traced requirements between the Business System Requirements Report Final and the System Integration and Test Plan, the System Integration and Test End of Test Completion Report shows the test results were not traced to the requirements, and the application did not execute all of the requirements as expected. The lack of consistent information regarding the effective execution of application requirements could impact the ability of the MeF system to perform the expected capabilities. In fact, during the first 3 weeks of operation, the MeF system rejected 29,697 (23 percent) of the 127,105 individual income tax returns filed.

We did not perform analyses to specifically determine whether the rejected individual income tax returns were directly related to the failed tests and identified defects. However, the TIGTA is currently conducting another audit to determine whether individual income tax returns transmitted through the MeF system are processed timely and accurately and in a manner consistent with tax returns processed in the current e-file system.



*Modernized e-File Will Enhance Processing of
Electronically Filed Individual Tax Returns, but
System Development and Security Need Improvement*

Recommendation

Recommendation 1: The Chief Technology Officer should ensure that project releases are deployed only after all system requirements are tested and met and that test results are verified to ensure their completeness and accuracy. If requirements are not met, defect reports should be prepared to allow for appropriate resolution by retesting or waiving the requirement prior to deployment.

Management's Response: The IRS disagreed with our recommendation. The IRS cited its milestone readiness review as a process for monitoring a project's progress toward satisfying exit conditions and for making formal go/no-go recommendations to the Executive Steering Committee. The Executive Steering Committee process provides the forum to discuss risk-based decisions prior to deployment of systems built and products delivered.

Office of Audit Comment: We acknowledge the controls the milestone readiness review and the Executive Steering Committee provide, and understand the role testing plays to ensure systems perform their intended functions accurately and reliably. However, with the significant number of failed tests reported and the subsequent problems with rejected individual income tax returns filed, we question whether the Executive Steering Committee had sufficient and timely information to make an informed risk-based decision for deploying MeF Release 6.1. As such, we continue to believe our recommendation to ensure that all system requirements are tested and met and results verified prior to deployment is valid and should be considered by the IRS.

Processing Valid Income Tax Returns for S Corporations – Form 1120S: In a prior TIGTA report entitled *Improvements to the Modernized e-File System Will Help Provide Intended Benefits to the Internal Revenue Service and Taxpayers*,⁶ we reported that as a result of MeF Release 4 processing the Modernized Tax Return Database and the Business Master File did not always agree on the taxpayer's entity information. Filing discrepancies occurred with the taxpayer's qualification to file a Form 1120, Form 1120S, or Form 1065 or with the tax periods reported by the taxpayer. Procedures were in place in the Submission Processing function to perfect tax return information sent from the Modernized Tax Return Database to the Business Master File. These procedures require correspondence with the taxpayer to resolve issues around the propriety of the tax return type necessary for filing.

However, we found that available front-end tax return validation controls are not being used to prevent inaccurate tax returns from being accepted by the MeF system. These controls notify taxpayers that they did not meet the qualifications for the entity or tax period used in filing and would need to file a different form. These controls prevent unnecessary tax return processing,

⁶ Reference Number 2008-20-122, dated June 18, 2008.



Modernized e-File Will Enhance Processing of Electronically Filed Individual Tax Returns, but System Development and Security Need Improvement

error resolution activity by the Submission Processing function, and correspondence with taxpayers.

We recommended that the Director, Submission Processing, and the Director, Electronic Tax Administration, perfect the validation controls to verify that taxpayers file the correct tax form based on their established filing election. These controls will prevent the MeF system from accepting the incorrect tax forms filed by taxpayers and, therefore, reduce the number of tax returns requiring Submission Processing function staff involvement. The IRS agreed with the recommendation for Form 1065 and Form 1120 and implemented the validation controls. The IRS proposed not implementing the validation controls for Form 1120S until processing and system limitations could be overcome.

Implementing controls to ensure acceptance of valid tax returns prevents unnecessary processing and correspondence by the IRS and unnecessary correspondence with taxpayers.

We followed up to determine the status of the corrective action for implementing the Form 1120S validation controls. The Wage and Investment Division's Submission Processing function informed us that the processing and system limitations for implementing the Form 1120S validation controls still exist. However, the Submission Processing function is planning to implement a solution to reduce the number of Form 1120S tax returns that are accepted and subsequently require further communication with the taxpayer regarding propriety of their current filing election.

The Modernized e-File Project Team Generally Followed Established Systems Development Processes, but Can Improve Its Management of Requirements and Risks

Our assessment of MeF Release 6.1 project management controls, that included project work breakdown structure schedules, task orders and modifications, and meeting minutes, found that adequate documentation was developed and maintained to meet Enterprise Life Cycle requirements. Additionally, the MeF Project Team adequately controlled and monitored funding for MeF Releases 6.1, 6.2, and 7. However, improvements to guidance in managing requirements and risks could have enhanced the project development schedule.

The MeF Project Team generally followed established systems development processes

The MeF Project Team adequately implemented the following management controls for developing Release 6.1.

Configuration Management: The configuration management plan addresses key items required by the Enterprise Life Cycle. The configuration management plan requires a repository for



*Modernized e-File Will Enhance Processing of
Electronically Filed Individual Tax Returns, but
System Development and Security Need Improvement*

project documentation and assigns responsibility for its maintenance and establishes a process for initiating and approving change requests.

Quality Management: The quality management plan adequately describes activities, roles, and responsibilities for the MeF quality assurance program. MeF Project quality examinations, customer technical reviews, and monthly contractor reports did not identify any issues or inconsistencies with planned quality assurance activities in the quality management plan.

Transition Management: MeF Release 6.1 development activities included end-user training plans, manuals, and organizational changes to provide adequate transition from system development to system operation. Reviews show that end-user manuals and related contact information was developed, and end-user training is on schedule.

Project Funding Management: The MeF Project Team properly controlled and monitored funding for MeF Releases 6.1, 6.2, and 7. Funding and scope changes were properly documented and approved for restructuring the MeF Project release schedule, as evidenced by documentation and meeting minutes from the IRS' MITS organization Enterprise Governance committee and Submission Processing Executive Steering Committee, the Department of the Treasury, and the Office of Management and Budget.

Funding realignments were properly controlled and approved. The Project required realignment of \$34 million from Release 7 to 6.1 to support unplanned and required needs including disaster recovery preparation and testing, the integration of processing and access with other applications and external users, and expanded hardware needs. This realignment was properly documented, controlled, and approved through the Submission Processing Executive Steering Committee.

The MeF Project funding also was the subject of several monthly MITS organization internal controls. These controls include the:

- Information Technology Project Control Review – assesses project progress and status in terms of management of cost, schedule, and technical complexity.
- Project Health Assessments – monitors risks associated with project management performance.
- Performance Measures Report – reports performance measures for both schedule and cost estimates at the project release and milestone level.

The MeF Project Team could have more effectively managed the risks associated with system capacity requirements

The MeF Project Team, in conjunction with the engineering organization, identified the need for appropriate infrastructure requirements early in Calendar Year 2008. As a result, a MeF system benchmark test was conducted in May 2008. The benchmark test results primarily included



*Modernized e-File Will Enhance Processing of
Electronically Filed Individual Tax Returns, but
System Development and Security Need Improvement*

development of performance measures needed to support the MeF Release 6 hardware architecture.

However, the Business Rules and Requirements Management office granted the MeF Project a waiver to exit the detailed design phase of the project development cycle in December 2008 without the final or new infrastructure requirements. The Business Rules and Requirements Management office granted the waiver because the MeF Project Team gave assurances they were working closely with the Infrastructure Architecture and Engineering office and were confident that any infrastructure changes would not negatively impact the project. The conditional approval to exit the detailed design phase was contingent upon the Business Rules and Requirements Management office receiving all final requirements by January 25, 2009. The detailed design phase exit was approved on December 4, 2008, without the revised infrastructure requirements.

In April 2009, the MeF Project Team formally identified capacity testing as a risk to the project schedule. This risk concerned the team's absence of experience in MeF system capacity testing for individual tax returns. Subsequently, the planned June 2009 system capacity testing was delayed and not completed until the end of September 2009. The capacity testing delay meant the final infrastructure requirements were not known until the end of September 2009.

The capacity testing results showed the infrastructure needed additional infrastructure hardware (eight Internet gateways) to securely manage the volume of electronic tax form transmissions for processing. The purchase and installation of these gateways is estimated to occur in March 2010 to handle the peak period of individual tax return filing in April. The cost for the infrastructure additions includes \$556,800 in hardware costs, \$355,453 for installation and configuration costs, and \$114,055 in related service costs for maintaining the gateways through January 2010. The additional infrastructure cost is \$1,026,308 of the total \$83.6 million estimated for the development and deployment of MeF Release 6.1.

The MITS organization's Risk Identification Procedure provides that special emphasis should be placed on risk identification during the planning stages of a project. In addition, the Risk Identification Procedure provides a checklist of risk categories and specific questions to consider during planning, including the following questions which may have helped the MeF Project Team identify capacity testing as a candidate risk:

- Has enough time been scheduled to design and implement unfamiliar areas?
- Will the product be operated in an unfamiliar or unproved software environment?
- Will the product be operated in an unfamiliar or unproved hardware environment?
- Are all of the technology requirements included in the enterprise architecture?
- Are there unique requirements that have never been implemented before?
- Is there customization required for hardware?



Modernized e-File Will Enhance Processing of Electronically Filed Individual Tax Returns, but System Development and Security Need Improvement

- Will infrastructure support groups be ready for deployment of products (including hardware, software licenses, and network support)?

After identification of candidate risks, the procedure also includes steps to guide the project to estimate the probable impact date of the risks, such as:

- Reviewing related program/project schedules and related information for impacted areas.
- As necessary, engaging the risk coordinator and other stakeholders and subject matter experts in determining the probable date of impact.
- Assessing date impacts of cross project and other external dependencies.
- Estimating and documenting a probable date when the candidate risk event could begin to negatively impact the program/project or organization entities.

By using the Risk Identification criteria previously cited, the issues encountered that delayed testing may have been addressed earlier in the development process. For instance, the Applications Development organization explained that capacity testing was delayed because the MeF focused capacity testing was not performed in the past and the Project Team was not prepared to meet the testing schedule. The complexity of this release and the potential volume of electronic tax form transmissions required a detailed test plan to ensure all necessary testing was identified. The organization also noted that technical issues were encountered with the test environment setup, components, and configurations, as well as tool license issues and data preparation problems. All of these issues required resolution to ensure successful testing.

The MeF Project Team may have avoided or reduced the risk associated with timely acquiring the additional infrastructure hardware needed had it applied lessons from prior release development and deployment experiences. In a prior TIGTA audit report entitled *The Modernized e-File Project Can Improve Its Management of Requirements*,⁷ we reported that the MeF system experienced problems in its ability to handle the number of returns filed during the March 2006 peak tax return filing period, and subsequently the Project Team developed lessons learned to address these problems and to prevent similar occurrences. Lessons learned from prior MeF releases that were not applied to validate MeF Release 6.1 included the need to timely validate performance engineering model assumptions and determine the impact of new forms and other processing loads on shared capacity.

Current guidance in the MITS organization Enterprise Life Cycle prescribes the development of a Lessons Learned Report at each milestone. However, we did not locate any guidance requiring the reference to or use of Lessons Learned Reports from prior phases or releases at the inception of new phases or releases of projects. The Phase Kickoff meeting directs an assessment of the detailed requirements, implementation approach (including tailoring plans), schedule, budget,

⁷ Reference number 2007-20-099, dated July 9, 2007.



Modernized e-File Will Enhance Processing of Electronically Filed Individual Tax Returns, but System Development and Security Need Improvement

risk and/or issues for that phase, and a revisit to the release strategy. However, this meeting does not require a review of Lessons Learned Reports as one of the items listed among the documents and other artifacts cited as inputs to the Project Initiation and Phase Kickoff Meeting Procedure.

The MeF Project Team identified that the risks in improperly sizing infrastructure hardware to help securely manage the volume of electronic tax form transmissions for processing may result in degrading system performance or even the inability to receive or view files for tax processing. The MeF Project Team also recognized the potential need for future expansion of the infrastructure hardware with procurement provisions for at least 16 more Extensible Markup Language gateways, if necessary.

The MeF system enhances the filing capabilities for tax preparers and the processing of tax returns for the IRS. These enhanced capabilities are not available if the MeF system is not operational. The MeF system is critical to States, which will not receive returns filed for them if it is not operational. Compromises of the MeF system's performance could affect the confidence taxpayers have in the IRS' ability to securely manage filed tax forms.

The use of Lessons Learned Reports is intended to improve the efficiency and effectiveness of future projects, releases, or phases by reducing the number of repeat issues and lessons already learned in the past.

Recommendations

The Chief Technology Officer should:

Recommendation 2: Modify the Enterprise Life Cycle guidance to require consideration of prior Lessons Learned Reports as part of the Project Initiation and Phase Kickoff Meeting Procedure in the early milestone planning stages.

Management's Response: The IRS agreed with our recommendation and will incorporate updates to the Project Initiation and Phase Kickoff Meeting Process Description and Procedure.

Recommendation 3: Use the Risk Identification Procedure as an input to the Enterprise Life Cycle's Project Initiation and Phase Kickoff Meeting Procedure.

Management's Response: The IRS agreed with our recommendation and will incorporate updates to the Project Initiation and Phase Kickoff Meeting Process Description and Procedure.



*Modernized e-File Will Enhance Processing of
Electronically Filed Individual Tax Returns, but
System Development and Security Need Improvement*

Modernized e-File Security Issues Were Not Adequately Controlled or Resolved

We assessed the security controls and issues related to the MeF Release 6.1 development. We reviewed the IRS MeF Release 6.1 System Security Plan for the inclusion of the security controls from the National Institute of Standards and Technology Special Publication 800-53, followed up on the resolution of the 13 MeF Release 4 security vulnerabilities previously reported on the MeF system, and monitored the MeF Release 6.1 detailed system design phase (Enterprise Life Cycle Milestone 4a) and additional system development phase (Enterprise Life Cycle Milestone 4b) exit condition security findings identified during the development of MeF Release 6.1.

While the IRS included the recommended security controls in the MeF System Security Plan, controls were not adequate to manage all of the security risks, issues, and action items. Although information provided by the IRS showed that 10 of the 13 security vulnerabilities were resolved by December 2008, the January 2010 Security Test and Evaluation reports that only 2 of the 13 vulnerabilities were resolved. Further, this Security Test and Evaluation identified two failed security controls that were not previously reported as vulnerabilities.

The MeF Project Team also reported resolving 12 of 15 security findings it identified during development. The three remaining findings relate to infrastructure, with imminent resolution of one finding and deferral of another to MeF Release 6.2; the last is considered outside the scope of the MeF application. Appendix V provides the details and status of actions to resolve the related weaknesses of the 13 security vulnerabilities and 15 security findings identified by the MITS organization.

The MeF System Security Plan included all of the recommended security controls

The MeF System Security Plan included all 212 of the National Institute of Standards and Technology Special Publication 800-53 (Revision 2) recommended security controls. Revision 3 to the Special Publication 800-53 was issued in August 2009. After consulting with the Department of the Treasury's Chief Information Security Officer, the IRS' Cybersecurity organization decided to implement this guidance with the Federal Information Security Management Act of 2002⁸ assessment that will begin in July 2010. Revision 3 includes 252 recommended security controls for the MeF that will be required for the next MeF release, scheduled for January 2011.

The MeF system successfully completed disaster recovery tests

Disaster recovery is an organization's ability to respond to an interruption in services by implementing a plan to restore critical business functions. The MeF system participated in

⁸ Pub. L. No. 107-347, Title III, 116 Stat. 2946 (2002).



*Modernized e-File Will Enhance Processing of
Electronically Filed Individual Tax Returns, but
System Development and Security Need Improvement*

disaster recovery testing on October 24, 2009. The tests showed that live transactions were successfully processed on the MeF disaster recovery environment and posted and stored to interfaced systems. Examples of the specific test accomplishments included:

- Successful processing of Internet filing and application-to-application transmissions.
- Successful tax return requests and displays through the Employee User Portal.
- Successful recovery of transactions from the disaster recovery site.
- Successful reverse replication showing query reports from the disaster recovery site and original database site were identical.

The Cybersecurity organization did not control or resolve all existing MeF security vulnerabilities

Security vulnerabilities are weaknesses identified in current operating systems. IRS policy specifies that all computer system weaknesses from any valid source should be entered in the *Plan of Action and Milestones* list. IRS system owners must track the status of the resolution of all weaknesses and verify that each weakness is corrected before reporting the item as resolved on the list.

The IRS is required to submit the *Plan of Action and Milestones* listing system weaknesses to the Department of the Treasury and the Office of Management and Budget on a quarterly basis. The Office of Management and Budget uses the information to assess the agency's progress in alleviating system weaknesses, monitor the Federal Government's ability to implement the Federal Information Security Management Act of 2002, and make budgetary decisions. Inaccurate or incomplete *Plan of Action and Milestones* information affects the Office of Management and Budget's ability to obtain an accurate status of IRS security weakness remediation.

There were 13 MeF system security vulnerabilities identified as part of the IRS Cybersecurity MeF Release 4 Security Risk Assessment, dated April 23, 2007. These security vulnerabilities were also reported in a prior TIGTA report entitled *The Internal Revenue Service Deployed the Modernized e-File System With Known Security Vulnerabilities*.⁹ Information provided about the status of the previously reported security vulnerabilities showed that in December 2008, 10 of the 13 vulnerabilities were resolved.

We performed an analysis of the vulnerabilities and found the resolution activity was not always adequately controlled or monitored. For example:

- *The processes for establishing and confirming user identification on the MeF system did not meet Federal Government standards for accrediting cryptographic modules.*

⁹ Reference Number 2009-20-026, dated December 30, 2008.



Modernized e-File Will Enhance Processing of Electronically Filed Individual Tax Returns, but System Development and Security Need Improvement

This vulnerability was initially tracked in the *Plan of Action and Milestones*, but was closed on December 3, 2007. On December 17, 2008, the IRS provided a management response to our report that showed that this issue was closed. On September 15, 2009, an Item Tracking Reporting and Control System risk was opened for this security vulnerability. The MITS organization is currently taking actions to resolve this vulnerability by March 15, 2010.

This vulnerability was not formally tracked by the IRS between the *Plan of Action and Milestones* being closed in December 2007 and the Item Tracking Reporting and Control System risk being opened in September 2009.

- Two security vulnerabilities for audit trails were not adequately controlled to reach resolution as part of Release 6.1 deployment:
 - *The MeF system and database have a number of audit log weaknesses, including 1) all required auditable events are not being captured, 2) no official has been assigned to monitor and maintain system audit mechanisms, 3) no database audit reduction tools were used, and 4) certain users that should have limited access have full capabilities to access database records, including taxpayer information.*
 - *An audit log review process was not in place, and logs were not being reviewed by MeF system officials.*

Both of these vulnerabilities were cancelled from the *Plan of Action and Milestones* on August 1, 2009, and were added to the IRS Security Material Weakness.¹⁰ Not all of the details for the cancelled security vulnerabilities were included in the material weakness. Additionally, based on the due dates of the material weakness, the security vulnerabilities will not be completed until between June 2010 and April 2011. Therefore, the security vulnerabilities may still exist for MeF Release 6.1 when it begins operating in February 2010. Additionally, the audit trail issue has been included in several prior TIGTA reports beginning in August 2004.¹¹

¹⁰ The IRS established the Security Material Weakness in 1997. Since then, the IRS has aggressively strengthened its computer security capabilities. The original 1997 plan was rewritten in 2003, 2005, and again in 2008. An Executive Steering Committee oversees the plan, ensuring that material weakness areas are addressed by all impacted organizations, appropriate policy and procedures are implemented, and actions resolve the systemic cause of the material weakness.

¹¹ *The Audit Trail System for Detecting Improper Activities on Modernized Systems Is Not Functioning* (Reference Number 2004-20-135, dated August 26, 2004), *Security Controls Were Not Adequately Considered in the Development and Integration Phases of Modernization Systems* (Reference Number 2005-20-128, dated August 18, 2005), *Improvements Are Needed to Ensure the Use of Modernization Applications Is Effectively Audited* (Reference Number 2006-20-177, dated September 29, 2006), and *The Internal Revenue Service Deployed Two of Its Most Important Modernized Systems With Known Security Vulnerabilities* (Reference Number 2008-20-163, dated September 24, 2008).



Modernized e-File Will Enhance Processing of Electronically Filed Individual Tax Returns, but System Development and Security Need Improvement

- *After the maximum number of consecutive unsuccessful login attempts, the MeF system did not enforce automatic account locks on user accounts for a minimum of 24 hours in accordance with IRS policies. The account lockout feature was set to 15 minutes.*

This security vulnerability was closed by the Cybersecurity office as part of a *Plan of Action and Milestones* item in April 2008. This vulnerability was subsequently reported to the Submission Processing Executive Steering Committee as a security finding in December 2009 (see Appendix V, Table 1 item 6 and Table 2 item 12). The vulnerability was not identified for resolution for approximately 20 months, when it was reported as a security finding. This security finding is currently open.

Subsequently, the January 2010 Security Test and Evaluation reports show that only 2 of the 13 security MeF system vulnerabilities were actually resolved. The Security Test and Evaluation also identified two failed security controls that were not previously reported as system security weaknesses. The failed controls involved user access limitations and configuration of audit trail record storage capacity.

Without proper controls to monitor and resolve the MeF system security vulnerabilities and findings, unauthorized access to taxpayer information would continue to be available and possibly go undetected. Consequently, the confidentiality, integrity, and availability of the taxpayer records maintained by MeF could be impacted. Also, weak supervision and review of user activities increases the opportunity for a user to perform undesirable actions that could go undetected by organization officials.

Controls were not adequately used to manage all security risks, issues, and action items affecting MeF Release 6 development

The MITS organization's Risk, Issue, and Action Item Management Directive establishes a common management process for addressing risks, issues, and action items across the MITS organization. A common management process promotes early identification and timely resolution of risks, issues, and action items when warranted. This Directive provides that:

- All programs/projects shall inventory and document risks, issues, and action items.
- All major and non-major projects, contractors, and stakeholders shall participate jointly and cooperatively in a common management process for risks, issues, and action items.
- All major and non-major projects shall record and maintain risk, issue, and action item data in a single, central repository.

Additionally, the Risk, Issue, and Action Item Management Process Description includes guidance for documenting the identification, assignment, and closure of risks, issues, and action items in a central repository.



Modernized e-File Will Enhance Processing of Electronically Filed Individual Tax Returns, but System Development and Security Need Improvement

The MeF Project charter assigns the project manager responsibility for assessing risks, which includes tracking risks until they are closed. Also, the MeF Project must adhere to the MITS organization's risk and issue management directive, process description, and procedures and use the Item Tracking Reporting and Control system for documenting and controlling risks and issues.

The MeF Project Team identified 10 security findings during MeF Release 6.1 development. These findings were controlled as one action item which required resolution to complete the detailed design stage of the release. Subsequently, the MeF Project Team identified five additional security findings during the release development activities. As of December 29, 2009:

- One Item Tracking Reporting and Control System ticket was opened to track the 10 detailed design stage security findings. Of these 10 findings, 8 have been closed, 1 is planned to be closed by March 2010, and 1 will be deferred for closure as part of MeF Release 6.2 in January 2011. The resolution to this finding is dependent upon the ability to successfully encrypt MeF information during data transmissions.
- Four of the five development stage security findings are not being tracked in the Item Tracking Reporting and Control System. Four have been closed and one is considered an "infrastructure" risk with resolution beyond the scope of the MeF system.

The MeF Project Team did not follow established MITS organization guidance for tracking of modernization project risks. The security findings were not related and not controlled individually in the Item Tracking Reporting and Control System. Absence of individual control of the findings may prevent management from obtaining the resolution status of the findings prior to the initiation of the release. If these risks are not resolved, the IRS may not be able to properly secure tax return information received through the MeF system.

The ability to adequately control the identification and resolution of security vulnerabilities and findings continues to challenge the IRS

TIGTA's report entitled *Customer Account Data Engine Release 4 Includes Most Planned Capabilities and Security Requirements for Processing Individual Tax Account Information*¹² found that improvement was needed in tracking vulnerabilities until resolution in the *Plan of Action and Milestones* list. Specifically, the IRS Cybersecurity organization does not monitor system owners' compliance with IRS policy to track all system vulnerabilities in the *Plan of Action and Milestones* lists. Further, it does not monitor system owners' compliance with IRS policy to verify that weaknesses are corrected before reporting them as resolved on the *Plan of Action and Milestones* list.

We recommended that the Chief Technology Officer direct the Cybersecurity organization to take actions that ensure the Customer Account Data Engine and mainframe computer system

¹² Reference Number 2009-20-100, dated August 28, 2009.



*Modernized e-File Will Enhance Processing of
Electronically Filed Individual Tax Returns, but
System Development and Security Need Improvement*

owners: 1) appropriately enter and track system vulnerabilities on control systems, including the *Plan of Action and Milestones* list and the Item Tracking Reporting and Control System, and 2) verify corrective actions are fully implemented before they are reported as resolved.

The IRS agreed with our recommendation. The corrective action stated that the Cybersecurity organization will continue to improve the process to ensure that system owners comply with IRS policy to enter and track all system vulnerabilities in IRS control systems. However, the lack of control of the MeF system vulnerabilities are continued evidence that the IRS needs to be more proactive in ensuring that system vulnerabilities are properly entered and tracked.

Recommendation

Recommendation 4: The Chief Technology Officer should ensure that the Cybersecurity organization will complete implementation of the process to ensure that system owners comply with IRS policy to enter and track all system security weaknesses in IRS control systems. This should include all MeF system security issues and it should be ensured they are monitored and tracked to resolution in either the *Plan of Action and Milestones* or the Item Tracking Reporting and Control System.

Management's Response: The IRS agreed with our recommendation. The Cybersecurity office responded that it has made continuous improvements to the *Plan of Action and Milestones* process in recent years and considers the process complete and implemented as of March 25, 2010.



*Modernized e-File Will Enhance Processing of
Electronically Filed Individual Tax Returns, but
System Development and Security Need Improvement*

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether the MeF Project Release¹ 6.1 development activities will provide the capability to electronically receive, process, and secure U.S. Individual Income Tax Returns (Form 1040), delivering the intended benefits to the IRS and taxpayers. This review was part of our Fiscal Year 2010 Annual Audit Plan for reviews of the IRS Business Systems Modernization efforts.

- I. Determined whether the MeF Project Release 6.1 development provides the planned capabilities and benefits to the IRS and taxpayers.
- II. Followed up on prior TIGTA report recommendations to determine whether the corrective actions for improvements to the MeF Project were adequate to resolve the issues regarding:
 - A. Implementation of controls to ensure only valid U.S. Income Tax Returns for an S Corporation (Form 1120S) are accepted for processing.
 - B. The use of bi-directional traceability for Release 6.1 requirements.
- III. Determined whether MeF Project Release 6.1 includes adequate security controls and whether all previously identified security vulnerabilities and findings have been resolved to provide adequate security of taxpayer return information on the MeF system.
- IV. Determined whether the MeF Project Releases 6.1, 6.2, and 7 funding and scope were properly monitored and controlled.

Modernized e-File Release 6.1 Requirement Samples

Tables 1 and 2 present the MeF Release 6.1 populations and samples we used to analyze the adequacy of the bi-directional requirement traceability (Subobjective II. B.). Table 1 presents the parameters of the sample we selected from the IRS customer requirements in the MeF Release 6.1, Milestone 4b, Business System Requirements Report to verify the requirements that were requested and approved for development were traced to system requirements.

Table 2 presents the parameters of the sample we selected of system requirements from the System Integration and Test Plan, Appendix A – Integration, Test, and Deployment Requirements Traceability Verification Matrix to verify that system requirements were considered for testing. The system requirements are developed in support of the IRS customer

¹ See Appendix VI for a glossary of terms.



*Modernized e-File Will Enhance Processing of
Electronically Filed Individual Tax Returns, but
System Development and Security Need Improvement*

requirements. Our samples included judgmentally selected requirements related to previously identified risks as well as randomly selected requirements for review. These samples enabled us to obtain sufficient evidence to support our results.

Table 1: Sample Selection of MeF Release 6.1 Customer Requirements From the Business System Requirements Report

<u>MeF Release 6.1 Customer Requirements Category</u>	<u>Sample Size From a Population of 361 Customer Requirements</u>
Security	2
Peak Processing	5
Authentication	1
Electronic Fraud Detection System	4
Every 36th Customer Requirement in the Business System Requirements Report	10
Total Sample Size	22

Source: Modernized e-File Release 6.1, Business System Requirements Report Final System Development Phase (Milestone 4b), dated December 3, 2009.

Detailed sample parameters:

- **Security** – We selected 2 MeF Release 6.1 customer requirements related to the security of the MeF system.
- **Peak Processing** – We selected 5 MeF Release 6.1 customer requirements related to the ability of the MeF system to support peak processing times.
- **Authentication** – We selected 1 MeF Release 6.1 customer requirement related to authentication of transmitters.
- **Electronic Fraud Detection System** – We selected 4 MeF Release 6.1 customer requirements related to the MeF system’s interface with the Electronic Fraud Detection System.
- **Every 36th Customer Requirement** – We randomly selected an additional 10 MeF Release 6.1 customer requirements.



Modernized e-File Will Enhance Processing of Electronically Filed Individual Tax Returns, but System Development and Security Need Improvement

Table 2: Sample Selection of MeF Release 6.1 System Requirements From the System Integration and Test Plan

<u>MeF Release 6.1 System Requirements Category</u>	<u>Sample Size From a Population of 250 System Requirements</u>
Capacity	5
Audit	7
Strong Authentication	2
Access Controls	5
Every 23rd System Requirement in the System Integration and Test Plan	10
Total Sample Size	29

Source: *Modernized e-File Release 6.1, System Integration and Test Plan, Appendix A - Integration, Test, and Deployment Requirements Traceability Verification Matrix, dated November 3, 2009.*

Detailed sample parameters:

- **Capacity** – We selected 5 MeF Release 6.1 system requirements related to the capacity of the infrastructure to support the MeF system.
- **Audit** – We selected 7 MeF Release 6.1 system requirements related to the ability of the infrastructure to produce audit records for the MeF system.
- **Strong Authentication** – We selected 2 MeF Release 6.1 system requirements related to the ability of the infrastructure to provide strong authentication of systems and users to the MeF system.
- **Access Controls** – We selected 5 MeF Release 6.1 system requirements related to the ability of the infrastructure to provide access controls for the MeF system.
- **Every 23rd System Requirement** – We randomly selected an additional 10 MeF Release 6.1 system requirements.

Internal controls methodology

Internal controls relate to management’s plans, methods, and procedures used to meet their mission, goals, and objectives. 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.



Modernized e-File Will Enhance Processing of Electronically Filed Individual Tax Returns, but System Development and Security Need Improvement

We determined the MeF Project's application development and security provisions provided the internal controls relevant to our audit objective. Specifically, this guidance includes the Enterprise Life Cycle,² the Internal Revenue Manual, and National Institute of Standards and Technology Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*. We assessed the adequacy of MeF Project development activities in relation to direction provided by this guidance. We also assessed the adequacy of MeF Project development and program plans by reviewing Business Systems Modernization program and project documentation and data provided by the IRS, the Business Systems Modernization Expenditure Plans, and the Exhibit 300, Capital Asset Plan and Business Case, required by the Office of Management and Budget. We supported this work by interviewing Applications Development organization, Wage and Investment Division, and Cybersecurity organization personnel.

² See Appendix IV for an overview of the Enterprise Life Cycle.



*Modernized e-File Will Enhance Processing of
Electronically Filed Individual Tax Returns, but
System Development and Security Need Improvement*

Appendix II

Major Contributors to This Report

Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)
Margaret E. Begg, Acting Assistant Inspector General for Audit (Security and Information Technology Services)
Scott A. Macfarlane, Director
Edward A. Neuwirth, Audit Manager
Mark K. Carder, Senior Auditor
Beverly K. Tamanaha, Senior Auditor
Louis V. Zullo, Senior Auditor



*Modernized e-File Will Enhance Processing of
Electronically Filed Individual Tax Returns, but
System Development and Security Need Improvement*

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Deputy Commissioner for Services and Enforcement SE
Commissioner, Wage and Investment Division SE:W
Associate Chief Information Officer, Applications Development OS:CTO:AD
Associate Chief Information Officer, Enterprise Services OS:CTO:ES
Director, Procurement OS:A:P
Director, Stakeholder Management OS:CTO:SM
Deputy Associate Chief Information Officer, Applications Development OS:CTO:AD
Deputy Associate Chief Information Officer, Systems Integration OS:CTO:ES:SI
Director, Test, Assurance, and Documentation OS:CTO:AD:TAD
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:
 Commissioner, Wage and Investment Division SE:W
 Associate Chief Information Officer, Applications Development OS:CTO:AD
 Director, Procurement OS:A:P
 Director, Program Oversight OS:CTO:SM:PO



*Modernized e-File Will Enhance Processing of
Electronically Filed Individual Tax Returns, but
System Development and Security Need Improvement*

Appendix IV

Enterprise Life Cycle Overview

The Enterprise Life Cycle¹ is the IRS' standard approach to business change and information systems initiatives. It is a collection of program and project management best practices designed to manage business change in a successful and repeatable manner. The Enterprise Life Cycle addresses large and small projects developed internally and by contractors.

The Enterprise Life Cycle includes such requirements as:

- Development of and conformance to an enterprise architecture.
- Improving business processes prior to automation.
- Use of prototyping and commercial software, where possible.
- Obtaining early benefit by implementing solutions in multiple releases.
- Financial justification, budgeting, and reporting of project status.

In addition, the Enterprise Life Cycle improves the IRS' ability to manage changes to the enterprise; estimate the cost of changes; and engineer, develop, and maintain systems effectively. Figure 1 provides an overview of the phases and milestones within the Enterprise Life Cycle. A phase is a broad segment of work encompassing activities of similar scope, nature, and detail and providing a natural breakpoint in the life cycle. Each phase begins with a kickoff meeting and ends with an executive management decision point (milestone) at which IRS executives make "go/no-go" decisions for continuation of a project. Project funding decisions are often associated with milestones.

¹ See Appendix VI for a glossary of terms.



*Modernized e-File Will Enhance Processing of
Electronically Filed Individual Tax Returns, but
System Development and Security Need Improvement*

Figure 1: Enterprise Life Cycle Phases and Milestones

Phase	General Nature of Work	Milestone
Vision and Strategy/ Enterprise Architecture Phase	High-level direction setting. This is the only phase for enterprise planning projects.	0
Project Initiation Phase	Startup of development projects.	1
Domain Architecture Phase	Specification of the operating concept, requirements, and structure of the solution.	2
Preliminary Design Phase	Preliminary design of all solution components.	3
Detailed Design Phase	Detailed design of solution components.	4A
System Development Phase	Coding, integration, testing, and certification of solutions.	4B
System Deployment Phase	Expanding availability of the solution to all target users. This is usually the last phase for development projects.	5
Operations and Maintenance Phase	Ongoing management of operational systems.	System Retirement

Source: *The Enterprise Life Cycle Guide*.



*Modernized e-File Will Enhance Processing of
Electronically Filed Individual Tax Returns, but
System Development and Security Need Improvement*

Appendix V

*Status of Resolution for Modernized e-File System
Security Vulnerabilities and Security Findings*

Table 1 presents the 13 MeF security vulnerabilities identified as part of the IRS Cybersecurity organization MeF Release¹ 4 Security Risk Assessment, dated April 23, 2007. Included is the status of the vulnerabilities provided by the IRS in response to a prior TIGTA report² and the status of the vulnerabilities as reported by the January 2010 Security Test and Evaluation.

Table 1: MeF Security Vulnerabilities

	Security Vulnerability	Vulnerability Status Provided by the IRS on December 17, 2008	Vulnerability Status As of January 2010
1	Unauthorized users had direct access to the MeF system management console, which provided system administrative functionalities such as the ability to change security settings and web services configurations. Any IRS employee with access to the Intranet could login to the console.	Resolved.	Resolved June 2007.
2	Security configuration settings on the MeF system servers and database were not sufficiently restrictive.	Resolved.	Unresolved.
3	Information input restrictions for State Government electronic tax filings were not in place on the MeF system.	Invalid and closed – resolved.	Unresolved.

¹ See Appendix VI for a glossary of terms.

² *The Internal Revenue Service Deployed the Modernized e-File System With Known Security Vulnerabilities* (Reference Number 2009-20-026, dated December 30, 2008).



*Modernized e-File Will Enhance Processing of
Electronically Filed Individual Tax Returns, but
System Development and Security Need Improvement*

	Security Vulnerability	Vulnerability Status Provided by the IRS on December 17, 2008	Vulnerability Status As of January 2010
4	The processes for establishing and confirming user identification on the MeF system did not meet Federal Government standards for accrediting cryptographic modules.	Resolved.	Unresolved.
5	Database users had more access privileges than they needed to carry out their responsibilities.	Resolved.	Unresolved.
6	After the maximum number of consecutive unsuccessful login attempts, the MeF system did not enforce automatic account locks on user accounts for a minimum of 24 hours in accordance with IRS policies. The account lockout feature was set to 15 minutes.	Unresolved.	IRS reported that solutions were implemented in production in April 2008; however, this same issue is listed as Security Finding 12 and is reported as an Infrastructure risk outside the scope of the MeF application.
7	Several database user accounts had multiple invalid password settings that were not in accordance with IRS policy.	Resolved.	Unresolved.
8	System users with limited access needs were granted full access to database records. Also, database administrator privileges were provided to nondatabase administrative personnel.	Resolved.	Unresolved.



*Modernized e-File Will Enhance Processing of
Electronically Filed Individual Tax Returns, but
System Development and Security Need Improvement*

	Security Vulnerability	Vulnerability Status Provided by the IRS on December 17, 2008	Vulnerability Status As of January 2010
9	The MeF system and database have a number of audit log weaknesses including 1) all required auditable events are not being captured, 2) no official has been assigned to monitor and maintain system audit mechanisms, 3) no database audit reduction tools were used, and 4) certain users that should have limited access have full capabilities to access database records, including taxpayer information.	Partially resolved, with the remaining actions to be completed in Fiscal Year 2009.	Unresolved.
10	An audit log review process was not in place, and logs were not being reviewed by MeF system officials.	Target completion date is December 31, 2008 – resolved.	Unresolved.
11	An alternate processing site agreement had not been established for the MeF system.	Resolved.	Resolved January 2008.
12	Business object reports containing personally identifiable information were transmitted in clear text.	Invalid and closed – resolved.	Unresolved.
13	System and database administrators used insecure methods to transmit MeF system data within the IRS.	Unresolved – To be resolved when MeF Release 5.5 deploys in January 2009.	Unresolved.

Source: Prior TIGTA report entitled The Internal Revenue Service Deployed the Modernized e-File System With Known Security Vulnerabilities (Reference Number 2009-20-026, dated December 30, 2008) and the January 2010 Security Test and Evaluation.



*Modernized e-File Will Enhance Processing of
Electronically Filed Individual Tax Returns, but
System Development and Security Need Improvement*

Table 2 presents 15 MeF system development security findings. The MeF Release 6 Project Team identified 10 security findings on December 8, 2008, during the detailed design stage of the release. Subsequently, the Project Team identified five additional security findings during the release development activities.

Table 2: MeF Security Findings

	Security Finding Description	IRS Reported Status As of December 29, 2009
1	User names and passwords are being transmitted in clear text.	Resolved June 2009.
2	Passwords are being generated by MeF on behalf of users. Passwords violate password complexity requirements.	Resolved December 2009.
3	Database credentials could be exposed to systems or network administrators.	Resolved December 2009.
4	Oracle auditing feature is not enabled in production and should be compliant for MeF Release 6.1.	Resolved December 2009.
5	The system fails to protect the integrity of transmitted data. Encryption is needed to support external sensitive but unclassified/personally identifiable information data transfers.	Resolved January 2009.
6	Insecure protocols, File Transfer Protocol, and Network File System are being used.	Resolved January 2009.
7	MeF Release 6 interface to Enterprise Application Integration Broker/National Account Profile is a new web service. Ensure new roles, data transfers, error handling, and provisioning of credentials are implemented securely.	Proposed resolution scheduled for Release 6.2 implementation January 2011.
8	The Disaster Recovery strategy for MeF Release 6.1 is not defined. An Enterprise Disaster Recovery Strategy is needed to properly address all components needed to address a recovery configuration for MeF Release 6.1.	Resolved November 2009.



*Modernized e-File Will Enhance Processing of
Electronically Filed Individual Tax Returns, but
System Development and Security Need Improvement*

	Security Finding Description	IRS Reported Status As of December 29, 2009
9	Business Objects used for statistical reporting. 1) Some reports are not adequately protected and marked "Sensitive But Unclassified"; 2) Auditing of business objects reports with "Sensitive But Unclassified" information is inadequate.	Resolved December 2009.
10	Gateway throughput of database not sufficient for peak loads for MeF Release 6.1.	Proposed Resolution scheduled for implementation March 2010.
11	Use of open source iText code presents a potential security risk.	Resolved January 2010.
12	After 3 unsuccessful attempts, the MeF system Web application and Web services automatically lockout the offending user accounts for only 15 minutes. The project office is currently verifying the 15 minutes and will confirm when confirmation is received.	The infrastructure risk is outside the scope of the MeF application. The proposed resolution is being tracked as a general support system issue.
13	Legacy Tax Return Data Base records for both U.S. Individual Income Tax Return (Form 1040) and Application for Automatic Extension of Time To File U.S. Individual Income Tax Return (Form 4868) contain National Account Profile data. Form 1040 records contain bank routing information which could be used for fraud by a corrupt administrator or inside attacker.	Resolved December 2009.
14	Application to application client application users and machine operators who send messages to the MeF system Web services cannot be individually identified, authenticated, and tracked by the MeF Release 6.1 system. Lack of individual accountability can encourage attackers to take advantage of the situation.	Resolved December 2009.
15	MeF Security Audit and Analysis System logs are not populated with two required fields. The two fields that were missing were the Error Code and Return Message.	Resolved December 2009.

Source: *The IRS Submission Processing Executive Steering Committee presentations.*



*Modernized e-File Will Enhance Processing of
Electronically Filed Individual Tax Returns, but
System Development and Security Need Improvement*

Appendix VI

Glossary of Terms

Term	Definition
Action Item	A short-duration, minimal resources activity assigned to a member or stakeholder in the program/project or organization within the MITS organization. An action item must be within the scope of the duties currently assigned to that person.
Business Objects	Objects in an object-oriented computer program that represent the entities in the business domain that the program is designed to support. For example, an order entry program might have business objects to represent each order, line items, and invoices.
Business Rule	A statement that defines or constrains some aspect of the business.
Business Systems Modernization	A complex effort that began in Calendar Year 1999 to modernize IRS technology and related business processes.
Capital Asset Plan and Business Case	Also known as Exhibit 300, it is used as a one-stop document for a myriad of information technology management issues such as business cases for investments, agency modernization efforts, and overall project management. The Office of Management and Budget requires each agency to submit an Exhibit 300 twice each year for each major information technology investment.
Customer Account Data Engine	Consists of databases and related applications that will replace the IRS official repository of taxpayer information (the Master File) and provide the foundation for managing taxpayer accounts to achieve the IRS modernization vision.
Database Credentials	Requirements for securely storing and retrieving database usernames and passwords for use by a program that will access a database.
Electronic Fraud Detection System	The primary information system used to support the IRS Criminal Investigation Division's Questionable Refund Program, which is a nationwide program established in January 1997 to detect and stop fraudulent and fictitious claims for refunds on income tax returns.
Employee User Portal	A web-hosting infrastructure that supports an Intranet portal that allows IRS employees to access business applications and data.



Modernized e-File Will Enhance Processing of Electronically Filed Individual Tax Returns, but System Development and Security Need Improvement

Term	Definition
Enterprise Application Integration Broker	A commercial off-the-shelf solution that will be used to enable the communication and data transformations between components of the Account Management Services system, the current processing environment, and the Customer Account Data Engine.
Enterprise Life Cycle	A structured business systems development method that requires the preparation of specific work products during different phases of the development process.
File Transfer Protocol	A standard set of rules used to exchange and manipulate files over a network, such as the Internet.
Governance	An IRS designed enterprise governance model that assigns all information technology projects to an appropriate executive oversight body.
Infrastructure	The fundamental structure of a system or organization. The basic, fundamental architecture of any system (electronic, mechanical, social, political, etc.) determines how it functions and how flexible it is to meet future requirements.
Issue	A situation or condition that either 1) currently has negative consequences for an Information Technology program/project or organization or 2) has 100 percent probability of having negative consequences for the program/project or organization.
Item Tracking Reporting and Control System	An information system used to track and report on issues, risks, and action items in the modernization effort.
iText	A library to create, read, or manipulate documents in the Portable Document Format. iText can export the same document to multiple formats or multiple instances of the same format.
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.
Milestone	Milestones provide for “go/no-go” decision points in a project and are sometimes associated with funding approval to proceed.



*Modernized e-File Will Enhance Processing of
Electronically Filed Individual Tax Returns, but
System Development and Security Need Improvement*

Term	Definition
MITIS Enterprise Governance Committee	The highest level recommending and decision-making body to oversee and enhance enterprise management of information systems and technology. It ensures strategic modernization and information technology program investments, goals, and activities are aligned with and support 1) the business needs across the enterprise and 2) the modernized vision of the IRS.
National Account Profile	A compilation of selected entity data from various Master Files. It includes all valid and invalid individual taxpayer entity information for all taxpayers on the Individual Master File, Business Master File, and Employee Plans Master File Processing.
National Institute of Standards and Technology	An agency under the Department of Commerce responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all Federal Government agency operations and assets.
Personally Identifiable Information	Information that can potentially be used to uniquely identify, contact, or locate a single person.
Portable Document Format	A fixed-layout document format used for representing two-dimensional documents in a manner independent of the application software, hardware, and operating system.
Release	A specific edition of software.
Requirement	A formalization of a need and the statement of a capability or condition that a system, subsystem, or system component must have or meet to satisfy a contract, standard, or specification.
Risk	A potential event that could have an unwanted impact on the cost, schedule, business, or technical performance of an Information Technology program/project or organization.
Security Test and Evaluation	A testing process that determines the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
Task Order	An order for services planned against an established contract.
Work Breakdown Structure	A deliverable-oriented grouping of project elements that organizes and defines the total scope of a project. A project schedule used to manage the tasks, task relationships, and resources needed to meet project goals.



*Modernized e-File Will Enhance Processing of
Electronically Filed Individual Tax Returns, but
System Development and Security Need Improvement*

Appendix VII

Management's Response to the Draft Report



CHIEF TECHNOLOGY OFFICER

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

RECEIVED
APR 21 2010

BY: *MS*

APR 21 2010

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Terence V. Milholland *Terence V. Milholland*
Chief Technology Officer

SUBJECT: Draft Audit Report – Modernized e-File Will Enhance Processing of
Electronically Filed Individual Tax Returns, but System Development
and Security Need Improvement (Audit #200920023) (i-trak #2010-
73931)

Thank you for the opportunity to review the draft audit report and respond to your assessments and observations. We appreciate the acknowledgement that the Modernization and Information Technology Services (MITS) organization included a plan to effectively manage the MeF system processing of the large volume of individual tax returns and requests for an extension to file on the MeF Release 6.1 deployment.

We would like to clarify that the MeF volume management plan was never intended to be a projection or commitment of how many tax returns transmitters would process through MeF since participation is voluntary for Filing Season 2010. The plan established volume limits or caps by transmitter in order to maintain system performance.

We are committed to continuously improving our information technology systems and processes. We value your continued support and the assistance and guidance your team provides. If you have any questions, please contact me at (202) 622-6800 or Karen Mayr at (202) 283-0015.



*Modernized e-File Will Enhance Processing of
Electronically Filed Individual Tax Returns, but
System Development and Security Need Improvement*

Attachment

Draft Audit Report - Modernized e-File Will Enhance Processing of Electronically Filed Individual Tax Returns, but System Development and Security Need Improvement (#200920023) (i-trak #2010-73931)

RECOMMENDATION #1: The Chief Technology Officer should ensure that project releases are deployed only after all system requirements are tested and met, and that test results are verified to ensure their completeness and accuracy. If requirements are not met, defect reports should be prepared to allow for appropriate resolution by retesting or waiving the requirement prior to deployment.

CORRECTIVE ACTION #1: We do not agree with this recommendation. One of the components in the Governance Layer of the ELC Framework is a Milestone Readiness Review. This is an ongoing monitoring of a project's progress toward satisfying exit conditions for the next Milestone Exit Review, and results in a formal go/no go recommendation to the Executive Steering Committee (ESC). The ESC process provides the forum to discuss risk-based decisions prior to deployment of systems built and products delivered.

IMPLEMENTATION DATE: N/A

RESPONSIBLE OFFICIAL: N/A

CORRECTIVE ACTION MONITORING PLAN: N/A

RECOMMENDATION #2: The Chief Technology Officer should modify the Enterprise Life Cycle guidance to require consideration of prior Lessons Learned Reports as part of the Project Initiation and Phase Kickoff Meeting Procedure in the early milestone planning stages.

CORRECTIVE ACTION #2: We concur with this recommendation. We will incorporate updates to the Project Initiation and Phase Kickoff Meeting Process Description and Procedure.

IMPLEMENTATION DATE: October 1, 2010.

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Services

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.



*Modernized e-File Will Enhance Processing of
Electronically Filed Individual Tax Returns, but
System Development and Security Need Improvement*

Attachment

Draft Audit Report - Modernized e-File Will Enhance Processing of Electronically Filed Individual Tax Returns, but System Development and Security Need Improvement (#200920023) (i-trak #2010-73931)

RECOMMENDATION #3: The Chief Technology Officer should use the Risk Identification Procedure as an input to the Enterprise Life Cycle's Project Initiation and Phase Kickoff Meeting Procedure.

CORRECTIVE ACTION #3: We concur with this recommendation. We will incorporate updates to the Project Initiation and Phase Kickoff Meeting Process Description and Procedure.

IMPLEMENTATION DATE: October 1, 2010.

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Services

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #4: The Chief Technology Officer should ensure that the Cybersecurity organization will complete implementation of the process to ensure that system owners comply with IRS policy to enter and track all system security weaknesses in IRS control systems. This should include all MeP system security issues and it should be ensured they are monitored and tracked to resolution in either the *Plan of Action and Milestones* or the Item Tracking Reporting and Control System.

CORRECTIVE ACTION # 4: We agree with this recommendation, in fact the Cybersecurity office has made continuous improvements to the Plan of Action and Milestones (POA&M) process in recent years, and now considers the process complete and implemented. With ongoing process improvements in place, the IRS considers this finding closed.

IMPLEMENTATION DATE: March 25, 2010

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.