Annual Assessment of the Internal Revenue Service Information Technology Program

September 28, 2012

Reference Number: 2012-20-120

ANNUAL ASSESSMENT OF THE INTERNAL REVENUE SERVICE INFORMATION TECHNOLOGY PROGRAM

Highlights

Final Report issued on September 28, 2012

Highlights of Reference Number: 2012-20-120 to the Internal Revenue Service Chief Technology Officer.

IMPACT ON TAXPAYERS

Successful modernization of IRS systems and the development and implementation of new Information Technology (IT) applications is necessary to meet evolving business needs. The IRS must ensure that its computer systems are effectively secured to protect sensitive financial and taxpayer data. The IRS also needs to ensure that it leverages viable technological advances as it improves its overall operational environment.

WHY TIGTA DID THE AUDIT

This audit was initiated as part of the TIGTA's Fiscal Year 2012 Annual Audit Plan and addresses the major management challenge of Modernization. TIGTA is required by the IRS Restructuring and Reform Act of 1998 to annually perform an evaluation of the adequacy and security of IRS technology.

WHAT TIGTA FOUND

Since last year's assessment, the IRS has developed and implemented significant systems, including the daily processing and database implementation projects of the Customer Account Data Engine 2 system and a new release of the Modernized e-File system. The daily processing project provides individual taxpayer account information to select downstream IRS systems on a daily basis and was implemented in January 2012. The database implementation project will establish a relational database that will store all individual taxpayer account data. It is in the testing phase and is expected to be placed into production in late 2012. Modernized e-File Release 7.0 was implemented in January 2012; however, plans to retire the Legacy e-File system in 2012 were revised.

TIGTA continues to believe that the IRS's Modernization Program remains a major risk. Improved controls are needed to ensure long-term success for two key systems within the Modernization Program. The development and implementation of new systems for Patient Protection and Affordable Care Act provisions present major IT management challenges. TIGTA suggests that the IRS continues to stress improvements in its overall control processes and performance, including implementing successful new systems, necessary to meet the IRS's mission-critical goals.

The IRS has made progress to improve information security and personnel safety; however, it needs to continue to place emphasis on information and physical security programs in order to ensure that policies, procedures, and practices adequately address security control weaknesses. Weaknesses were identified over system access controls, configuration management, audit trails, physical security, remediation of security weaknesses, and oversight and coordination on security-related issues. Until the IRS addresses security weaknesses, it will continue to put the confidentiality, integrity, and availability of financial and taxpayer information and employee safety at risk.

The IRS IT organization envisions becoming a world-class provider of IT services by focusing on its people, processes, and technology. It implemented virtualization technology to continue to improve operational efficiency, but additional improvements are needed. In addition, the IT organization is effectively working human capital issues, but improvements are needed there also.

WHAT TIGTA RECOMMENDED

Because this was an assessment report of the IRS's IT Program through Fiscal Year 2012, TIGTA did not offer any recommendations. IRS officials were provided with an opportunity to review and comment on the report.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 28, 2012

MEMORANDUM FOR CHIEF TECHNOLOGY OFFICER

FROM: Michael E. McKenney
Acting Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Annual Assessment of the Internal Revenue Service Information Technology Program (Audit # 201220010)

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 perform an evaluation of the adequacy and security of the technology of the IRS since August 1, 2011, as required by the IRS Restructuring and Reform Act of 1998.[1] This audit is included in the Treasury Inspector General for Tax Administration's Fiscal Year 2012 Annual Audit Plan and addresses the major management challenge of 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.).

Table of Contents

Background ..... Page 1

Results of Review ..... Page 6

Systems Modernization and Applications Development Background ..... Page 6

Improved Controls Are Needed to Ensure Long-Term Success for Two Key Systems Within the Modernization Program ..... Page 8

Achieving Program Efficiencies and Cost Savings ..... Page 12

Development and Implementation of New Systems for the Patient Protection and Affordable Care Act Provisions Present Major Information Technology Management Challenges ..... Page 13

Information Security Background ..... Page 15

Progress Is Being Made to Improve Information Security and Personnel Safety ..... Page 16

Continued Management Attention Is Needed to Address Weaknesses in Information and Physical Security ..... Page 18

Information Technology Operations Background ..... Page 24

Information Technology Operational Efficiency Continues to Improve, but Additional Improvements Are Needed ..... Page 24

The Information Technology Organization Is Effectively Working Human Capital Issues, but Additional Improvements Are Needed ..... Page 25

Appendices

Appendix I – Detailed Objective, Scope, and Methodology ..... Page 29

Appendix II – Major Contributors to This Report ..... Page 30

Appendix III – Report Distribution List ..... Page 31

Appendix IV – List of Treasury Inspector General for Tax Administration Reports Reviewed ..... Page 32

Appendix V – Number of Internal Revenue Service Information Technology Employees ..... Page 35

Appendix VI – Glossary of Terms ..... Page 36

Abbreviations

ACA	Patient Protection and Affordable Care Act
ACIO	Associate Chief Information Officer
CADE 2	Customer Account Data Engine 2
CTO	Chief Technology Officer
e-File	Electronic Filing
EUES	End User Equipment and Services
FY	Fiscal Year
GAO	Government Accountability Office
IRDM	Information Reporting and Document Matching
IRS	Internal Revenue Service
IT	Information Technology
MeF	Modernized e-File
TIGTA	Treasury Inspector General for Tax Administration

Background

The Internal Revenue Service (IRS) Restructuring and Reform Act of 1998[1] requires the Treasury Inspector General for Tax Administration (TIGTA) to evaluate the adequacy and security of the IRS's Information Technology (IT) Program annually. This report provides our assessment of the IRS's IT Program and its operations for Fiscal Year (FY)[2] 2012.

Each year, the IRS collects more than $2 trillion in tax revenue and manages about 220 million individual taxpayer accounts and more than 40 million business taxpayer accounts.[3] The IRS receives as many as 20 million inquiries from taxpayers during the peak week of the filing season. Further, the Federal tax code includes more than 44,000 pages and is updated based on more than 200 tax law changes enacted each year. According to the Draft IRS IT Business Plan FYs 2011–2013, the primary business challenges that the IRS faces include:

- Increasing complexity of tax administration due to the breadth of existing tax laws and annual tax code changes from new legislation.
- Growing human capital challenges due to an aging staff and 39 percent of its executives nearing retirement.
- Keeping up with the explosion in electronic data with online interactions and related security risks as technologically perceptive taxpayers and employees are increasingly using online tools.
- Accelerating globalization from increasing taxpayer and corporate foreign income requires experience and tools in international tax administration.
- Expanding role of tax practitioners and other third parties in the tax system as individuals increasingly use outside help, such as tax preparers and software.
- Maintaining the technology of the legacy systems used to perform core IRS processes, which will require effort and skill.
- Complying with the mandate to ensure the security and privacy of taxpayer personal and financial information, IRS infrastructure, and IRS applications.
- Improving operational efficiency amid increasing budget constraints by optimizing existing technology and prudently planning future technology.

[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.).
[2] See Appendix VI for a glossary of terms.
[3] IRS IT Draft Business Plan FYs 2011–2013.

The IRS reported that the 2012 Filing Season was a key turning point in modernizing the IRS technology infrastructure and instituting processes to deliver outstanding tax administration services to the American public.[4] To align with these milestones, effective July 1, 2012, the Modernization and Information Technology Services organization changed its name to the IRS Information Technology organization. The IRS reports that the name change reflects a shift in the organization's way of thinking and operating as it collaborates with the business and functional operating divisions to deliver the IRS's mission. Instead of modernization being treated as a separate and distinct strategic offering within the IRS IT organization, it will now be incorporated into the overall portfolio.

The IRS Chief Technology Officer (CTO) is responsible for advising the Commissioner on all IT matters, managing the IRS's information system resources, and delivering and maintaining modernized information systems throughout the IRS. The following Associate Chief Information Officer (ACIO) offices support the CTO:

- Applications Development is responsible for building, testing, delivering, and maintaining integrated software solutions to support modernized systems that manage taxpayers' accounts, interactions with taxpayers, and potential audit and collection activities.
- Enterprise Services is responsible for strengthening the technology infrastructure across the enterprise and for defining how the enterprise-wide data environment is organized, identified, shared, and reused.
- Strategy and Planning is collaborating with IT leadership and external stakeholders to provide policy, direction, and administration of essential programs. Strategy and Planning ensures selection, planning, and management of an IT investment portfolio.
- End-User Equipment and Services (EUES)[5] provides IT products and support services to IRS end-users. It is the single point of accountability for personal computing, help desk support, asset management, local area networks, and telephone communications support.
- Enterprise Networks manages the design and engineering of the IRS's telecommunications environment and is responsible for developing the long-range enterprise network strategy and managing telecommunications projects.
- Enterprise Operations supports the mainframe and server environment for all IRS business entities and taxpayers. Enterprise Operations is developing the new enterprise-wide development and test environment and is establishing maximum security management.

[4] IRS Name Change Guidance dated June 28, 2012.
[5] On April 22, 2012, the EUES organization merged with the Enterprise Networks organization to form the User and Network Services organization.

- Cybersecurity ensures 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.
- Affordable Care Act Program Management Office is responsible for managing the strategic planning, development, and implementation of new information systems supporting IRS business requirements under provisions of the Patient Protection and Affordable Care Act (ACA).[6]
- Management Services works with information technology leadership to define and implement human capital policies and guidance.
- The Modernization Program Management Office leads the Customer Account Data Engine 2 (CADE 2) system development efforts.

The IRS IT organization's FY 2012 budget was more than $2.1 billion, of which $330.21 million was for Business Systems Modernization. The IRS appropriations language in H.R. 2055,[7] dated January 5, 2011, specifies that the IRS Business Systems Modernization program include the CADE 2 and Modernized e-File (MeF) systems' investments. Figure 1 provides a breakdown of the FY 2012 budget supporting the IRS IT organization by specific funds.

[6] Pub. L. No. 111-148, 124 Stat. 119 (2010) (codified as amended in scattered section of the U.S. Code), as amended by the Health Care and Education Reconciliation Act of 2010, Pub. L. No. 111-152, 124 Stat. 1029.
[7] Consolidated Appropriations Act, 2012, H.R 2055-103, 112th Cong. (2012).

Figure 1: IRS Information Technology FY 2012 Budget by Fund

IRS Information Technology	Operations Support ACIOs FY 2012 Budget	FY 2012 Budget
Applications Development	$458,812,276	
Enterprise Services	$63,041,742	
Strategy and Planning	$42,439,223	
User and Network Services	$429,600,475	
Enterprise Operations	$351,076,320	
Cybersecurity	$129,221,937	
Other Associate Chief Information Officers (ACIO)	$334,034,859	
Total Operations Support Fund		$1,808,226,832
Affordable Care Act Fund		$33,838,291
Business Systems Modernization Fund		$330,210,000
Return Preparer Initiative Fund		$681,527
User Fees Fund		$220,000
Reimbursable Fund		$4,469,311
Total IRS Information Technology FY 2012 Budget		**$2,177,645,961**

Source: IRS IT, Strategy and Planning ACIO, Financial Management Services, February 2012.

As of June 30, 2012, the IRS IT organization employed 7,228 individuals. Appendix V provides a breakdown of the number of IRS IT employees by their respective functions. As of May 30, 2012, the IRS IT organization also employed almost 2,000 contractors.

The compilation of information for this report was conducted at the TIGTA office in Atlanta, Georgia, during the period June through August 2012. We considered TIGTA reports issued to the IRS between August 1, 2011, and September 30, 2012,[8] as well as reviewed relevant reports published by the Government Accountability Office (GAO), IRS Oversight Board, National Taxpayer Advocate, and the IRS. In addition, we considered congressional testimonies.

[8] Please see Appendix IV for a list of TIGTA audit reports used in this assessment.

Our audit work was 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. 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.

Results of Review

Systems Modernization and Applications Development Background

The Business Systems Modernization Program (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. Successful modernization of IRS systems and the development and implementation of new IT applications is necessary to meet evolving business needs. The IRS budget for FY 2012 includes $330.21 million to remain available until September 30, 2014, for "necessary expenses of the Internal Revenue Service's business systems modernization program." Such expenses include the capital asset acquisition of information technology systems, including management and related contractual costs of said acquisitions (and related IRS labor costs) and contractual costs associated with authorized operations.

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. Goals for the Modernization Program include the following:

- Issuing refunds, on average, five days faster than existing legacy systems.
- Offering electronic filing (e-file) capability for individuals, large corporations, 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.

Last year was the first year since 1995 that the IRS did not identify and report the Modernization Program as a material weakness under the Federal Financial Management Improvement Act.[9] In June 2011, the IRS Commissioner certified, in a memorandum to the Department of the Treasury's Assistant Secretary for Management and Chief Financial Officer, that the internal and management control weaknesses contributing to the material weakness had been fully addressed. Based on achievements at that time, the IRS concluded that issues raised related to the early

[9] Pub. L. No. 97-255 – (H.R. 1526).

modernization programs and the management processes and controls in place for the Modernization Program were no longer a material weakness for the IRS. While we supported the IRS's decision last year based on the accomplishments and preliminary results at the time, based on our current assessment of the IRS's IT Program, we believe the Modernization Program remains a major risk. Further, we suggest that the IRS continue to stress improvements in its overall control processes and performance, including developing and implementing successful new systems and applications that are necessary to meet IRS's mission-critical goals and capabilities.

In June 2012, the GAO reported[10] that the IRS's challenge in addressing its material weakness in internal controls over unpaid assessments resulted from three specific control deficiencies: (1) inability to rely on its general ledger and underlying subsidiary records to report in accordance with Federal accounting standards without significant compensating procedures; (2) inability to trace reported taxes receivable to supporting transactions and maintain an effective transaction-based subledger for unpaid assessment transactions; and (3) inability to effectively prevent or timely detect and correct errors in taxpayer accounts. In its report, the GAO concluded that these conditions were caused "primarily by IRS's continued reliance on software applications that were not designed to provide accurate, complete, and timely transaction-level financial information, as well as errors in taxpayer accounts." Further, the GAO stated, "These problems are likely to continue to exist until these software applications are either significantly enhanced or replaced, and IRS remedies the control deficiencies that continue to result in significant errors in taxpayer accounts."

The IRS Oversight Board recently stressed the importance of the IRS Modernization Program and emphasized the continuing need for a modern IT system as the foundation for major increases in IRS efficiency and reduced taxpayer burden through Electronic Tax Administration.[11] The Oversight Board's vision for Electronic Tax Administration is a tax administration system that provides secure, convenient, timely, and accurate services to taxpayers and to the tax professionals and IRS employees who serve them. The Oversight Board has approved two long-term goals that it uses to measure the IRS's progress in modernizing itself: (1) the rate at which taxpayers electronically file their tax returns and (2) the successful and timely delivery of the CADE 2 and MeF systems.

The IRS's National Taxpayer Advocate reported to Congress that:

> *CADE 2 is expected to resolve many computational problems. Beginning January 2012, the IRS will roll out an extensive system modernization known as CADE 2, that will permit the Individual Master File to accept and post taxpayer account updates every business day. Instead of waiting two weeks for payments to post, it will only take from*

[10] GAO, GAO-12-695, *Status of GAO Financial Audit and Related Financial Management Recommendations*, pp. 7–8 (June 2012).
[11] IRS Oversight Board Annual Report to Congress 2011, p. 37 (May 2012).

> *48 hours to a week. Ultimately, CADE 2 will replace the more than 50-year-old system the IRS now uses to process tax return data. The new database and its related applications will, over time, replace the IMF [Individual Master File] and the BMF [Business Master File] as the IRS system of record for taxpayer accounts and will speed the transition from the multiple systems that now manage taxpayer accounts to one comprehensive system. The IRS anticipates that the January 2012 release of CADE 2 and the availability of real-time data will eliminate some account [sic] restricting for interest and certain interest accruals and will increase timeliness of taxpayer account data. For this reason, it is important that CADE 2 continue to develop, roll out, and operate as planned.*

At that time, the National Taxpayer Advocate also recognized that the IRS had recently implemented several technology enhancements that can assist taxpayers to obtain information more easily. This includes a new phone application, IRS2Go, which can be downloaded to a smartphone for free. Taxpayers can use IRS2Go for a number of things, including checking the status of their tax refund and subscribing to tax tips.

Improved Controls Are Needed to Ensure Long-Term Success for Two Key Systems Within the Modernization Program

MeF system

The MeF system is a critical component of the IRS initiative to meet the needs of taxpayers, reduce taxpayer burden, and broaden the use of electronic interactions. Unresolved performance issues with MeF Release 7.0 and planned Calendar Year 2012 infrastructure changes for the IRS have impaired efforts to retire the existing Legacy e-File system and delayed plans for receiving employment tax forms through MeF Release 8.0.[12]

Over the last calendar year, the IRS took important steps to increase the volume of returns transmitted to the MeF system and increased the number of vendors' software packages available to transmit electronic tax returns. However, our audit found that unresolved performance issues with MeF Release 7.0 existed as of its deployment. In addition, the IRS IT organization is planning significant infrastructure changes in Calendar Year 2012 that will introduce uncertainty and may affect the MeF system's reliability. Further, the IRS has not developed a retirement plan for the existing Legacy e-File system, including measurable shutdown conditions for that system, even though it was scheduled to be retired in October 2012. Finally, the MeF system has not yet fully demonstrated the ability to process all electronically filed returns for a filing season, projected to be more than 121 million combined individual and business returns.

To address these findings, we recommended that the CTO: (1) advise the Wage and Investment Division to defer the retirement of the Legacy e-File system until the increased risk associated

[12] See Appendix IV, Reference Number 2012-20-121.

with retiring the system can be addressed; (2) update the Internal Revenue Manual to include improved performance testing processes, ensure system performance test teams obtain approved waivers or deferrals when performance tests are not executed, and ensure performance test teams submit End of Test Status Reports for senior management review; and (3) advise the Wage and Investment Division to complete a retirement plan for the Legacy e-File system, as well as communicate retirement milestones and a timeline to key stakeholders.

In their response to the report, IRS officials partially agreed with the recommendations. The IRS plans to develop a contingency plan for the MeF system and to update the Internal Revenue Manual as needed. The IRS has also revised its timeline to retire the Legacy e-File system. However, IRS management did not concur with our recommendation to develop a retirement plan for the Legacy e-File system that includes associated implementation dates and monitoring processes.

CADE 2 system

The January 2012 implementation of the CADE 2 system daily processing capabilities, which provide individual taxpayer account information to downstream IRS systems on a daily basis, enabled the IRS to process tax returns for individual taxpayers more quickly by replacing existing weekly processing. This key modernization system will include a centralized database of individual taxpayer accounts, allowing IRS employees to view tax data online and provide timely responses to taxpayers. The successful implementation of the CADE 2 system is intended to significantly improve services to taxpayers and significantly enhance IRS tax administration.

The IRS initiated systems development testing of the CADE 2 system, reduced the risks to the filing season by implementing independent contractor recommendations, and performed simulated exercises to identify potential issues that could occur during the filing season. However, we found that improvements are needed in key controls and processes for requirements management, process testing, and security testing to ensure the long-term success of the CADE 2 system.[13] TIGTA recommended that the CTO take necessary steps to ensure:

- Test cases and other appropriate documentation are properly developed for infrastructure requirements.
- All infrastructure documentation includes complete traceability to the requirements being tested and the testing results.
- IRS testers obtain and maintain documentation to verify test results.
- Test execution practices are consistent.
- All system security requirements and corresponding test cases are identified and sufficiently traced, managed, and tested.

[13] See Appendix IV, Reference Number 2012-20-122.

- All database issues identified by vulnerability scanning are resolved or an action plan is developed with specific corrective actions and associated time periods for completion.
- All issues identified by source code security review scans are resolved and an action plan is developed with specific corrective actions and associated time periods for completion prior to the code being placed into service.

In management's response to the report, the IRS partially disagreed with three of our eight recommendations. The IRS disagreed with developing an enterprise-wide program-level Requirements Traceability Verification Matrix and policy. We believe, however, that an enterprise-wide approach is needed to strengthen oversight of traceability controls. Also, the IRS stated that automated tools are not always needed for control of requirements and test case management for IT systems development. We maintain that the use of one suite of integrated automated tools would provide needed control over volumes of requirements and test cases for IRS systems, including the monumental CADE 2 systems development initiative. Lastly, the IRS responded that additional CADE 2 documentation is not needed to ensure complete traceability of requirements to test results. Specifically, the IRS stated that adequate documentation already exists with Government Equipment Lists and environmental checklists. However, as stated in our report, while this documentation does verify infrastructure components have been acquired and implemented, it does not verify that all CADE 2 processing requirements have been tested.

Further, it is critical for the IRS to accurately execute, monitor, and assess performance and capacity testing for the CADE 2 because these controls directly affect whether, after implementation, the system will be capable of processing the necessary quantity and types of information within required time periods. This is needed to avoid possible delays with taxpayer refunds and degraded customer service. As part of the CADE 2 systems development process, the IRS established a testing environment for the CADE 2 system that was representative of the existing production environment. This approach allowed the IRS to obtain meaningful data from its preproduction tests. However, the IRS did not follow procedures to ensure that performance requirements were completely tested during the Final Integration Test Phase I.[14] As a result, the IRS may not have acquired all the necessary information to make a fully informed decision on the ability of the CADE 2 system to effectively process transactions under expected normal and peak workload conditions within acceptable response time thresholds. To address specific control weaknesses with system performance testing, we recommended that the ACIO, Applications Development, take steps to ensure internal controls for testing performance and capacity requirements are formally and effectively implemented to ensure the traceability of these requirements through the performance testing process.

One of the primary goals of the CADE 2 system is for it to be a trusted source of data for the IRS and taxpayers. To provide this, the system requires a stable design to support tax processing

[14] See Appendix IV, Reference Number 2012-20-051.

functions and ensure complete and accurate data. The database implementation project will establish a relational database that will store all individual taxpayer account data. It is currently in the testing phase and is expected to be placed into production in late 2012. However, we determined that data integrity testing completed did not provide assurance that CADE 2 system data are consistently accurate and complete.[15] Also, the CADE 2 system database design has not fully met initialization, daily update, and downstream interface needs. In June 2012, the IRS acknowledged that it was having problems with its CADE 2 system database interface to the Integrated Data Retrieval System Taxpayer Information File. As a result, the IRS is reevaluating its data strategy for feeding downstream systems and is considering delaying the interface. The IRS spent about $22.3 million on database implementation, which included developing Version 2.2 of the CADE 2 database. However, the IRS does not track cost at the development activity level and, consequently, we could not determine the actual cost for the new version of the CADE 2 database. Enhanced security is also a primary goal for the CADE 2 system. However, vulnerabilities in the JAVA code could result in loss of sensitive taxpayer information.

The IRS agreed with three and partially agreed with one of the seven recommendations, and corrective actions are planned. However, the IRS disagreed with three of our recommendations to: (1) ensure that the database design process follows the Internal Revenue Manual and validate that the database design meets business requirements, (2) realign data validation and testing efforts with business functionality and processes, and (3) disable or remove sample tables and default ports prior to the CADE 2 Program exiting Transition State 1. The IRS believes that its current development and testing processes are sufficient to address recommendations 1 and 2. For recommendation 3, the IRS will consider changing the default port as part of an enterprise risk mitigation remediation plan, while the IRS management's response is silent on what actions, if any, the IRS will take regarding sample tables.

A final matter for careful consideration regarding the CADE 2 system is an announcement[16] from the CADE 2 Governance Board in July 2012. The announcement noted that in January 2012, the IRS made history, delivering a daily processing capability for individual taxpayers after 50+ years on a weekly cycle. The announcement also highlighted that in March 2012 the IRS "delivered a new state-of-the-art database, loaded with over 270 million taxpayer accounts and over a billion tax modules" as an "immediate leap forward for the IRS from a technology standpoint." However, the Governance Board also stated "there is much more to be done, and now more than ever, we need all hands on deck to reach our September delivery for Database Implementation." Despite several specific progress areas for the CADE 2 system that are noted in the Board's announcement, the IRS openly acknowledged that "the program has also experienced delays across Database Implementation, and there is a clear risk of further schedule delays."

[15] See Appendix IV, Reference Number 2012-20-109.
[16] Message from the Governance Board: CADE 2 Database Implementation (July 2, 2012).

The following specific challenges and risk mitigation strategies for the CADE 2 system were identified by the IRS as being underway:

- Establishing clarity around points of accountability, integration, and priorities for the various functions and key players to help meet the September 2012 deliverable, with expanded leadership from the Program Management Office to drive those accountabilities.
- Addressing resources, both personnel and hardware, that can be reallocated to the highest priorities for the September 2012 deployment.
- Instituting working norms to rationalize meeting attendance and reduce fragmentation of employee focus.
- Rapidly updating, communicating, and maintaining an accurate high-level schedule to facilitate decision making as changes in progress occur.
- Incorporating several broader lessons learned with CADE 2 system execution.

Achieving Program Efficiencies and Cost Savings

Given the current economic environment and the increased focus by the Administration, Congress, and the American people on Federal Government accountability and efficient use of resources, the American people must be able to trust that their Government is taking action to stop wasteful practices and ensure that every tax dollar is spent wisely. This major management challenge relates directly to IT capital planning and investment management controls for the IRS's systems and applications. As part of our annual assessment of the status of the IRS's IT Program, we considered the following information and reports that demonstrate the need for improvements in program efficiencies.

The IRS FY 2012 budget includes $330.21 million to remain available until September 30, 2014, for "necessary expenses of the Internal Revenue Service's business systems modernization program." Such expenses include the capital asset acquisition of information technology systems, including management and related contractual costs of said acquisitions (and related IRS labor costs) and contractual costs associated with authorized operations. The Consolidated Appropriations Act of 2012 specifically requires the IRS to submit a quarterly report to the House and Senate Committees on Appropriations and the Comptroller General of the United States detailing the cost and schedule performance for the CADE 2 system and the MeF system IT investments. The report should include the purposes and life-cycle stages of the investments, the reasons for any cost and schedule variances, the risks of such investments and the strategies the IRS is using to mitigate such risks, and the expected developmental milestones to be achieved and costs to be incurred in the next quarter.

We reviewed, but did not verify, the quarterly status information provided by the IRS in accordance with the previously discussed budget provisions. In its most recent quarterly submission, the IRS included cost and schedule performance information for the CADE 2 and MeF programs as well as five other programs, as specified by the Act. The five other IRS programs currently being tracked quarterly under the 2012 Modernization Program budget provisions are the:

- Enterprise Data Access Strategy/Integrated Production Model.
- E-Services.
- Information Reporting and Document Matching (IRDM).
- IRS.gov.
- Return Review Program.

In January 2012, the GAO reported[17] on weaknesses associated with the implementation of sound cost-estimating practices for IRS systems. In its report, the GAO concluded that the IRDM's 2011 cost estimate, used to justify the program's projected budgets of $115 million for FYs 2012 through 2016, generally does not meet best practices for reliability. The GAO review found that the cost estimate minimally meets best practices for a well-documented estimate because the IRS did not provide detailed support for staff resources and the cost estimate documentation justified only about six out of the 86 requested Full-Time Equivalent staff for the IRDM, among other things. If documentation does not provide source data or cannot explain the calculations underlying the cost elements, the estimate's credibility may suffer. Also, the IRDM program's earned value management data did not meet data reliability criteria in the areas GAO reviewed. Specifically, the IRDM project schedule was not properly sequenced, meaning activities were not properly linked in the order in which they were to be carried out. In addition, surveillance was not conducted on the IRDM's earned value management system, as required by the Office of Management and Budget and the Department of the Treasury. Surveillance involves having qualified staff review an earned value management system. The GAO concluded that because the IRDM's 2011 cost estimate is based on unreliable earned value management data, it does not provide adequate support for the IRDM's budget requests.

Development and Implementation of New Systems for the Patient Protection and Affordable Care Act Provisions Present Major Information Technology Management Challenges

The ACA contains an extensive array of tax law changes that will present a continuing source of challenges for the IRS in the coming years. While the Department of Health and Human Services will have the lead role in the policy provisions of the ACA, the IRS will administer the

[17] GAO, GAO-12-59, *Cost Estimate for New Information Reporting System Needs to Be Made More Reliable* (Jan. 2012).

law's numerous tax provisions. The IRS estimates that at least 42 provisions will either add to or amend the tax code and at least eight will require the IRS to build new processes that do not exist within the current tax administration system. In addition, the IRS must create new or revise existing tax forms, instructions, and publications; revise internal operating procedures; and reprogram major computer systems used for processing tax returns.

To address this emerging IT Program risk area, our annual IT assessment considered the broader planning efforts underway in response to emerging legislative requirements for the IRS under the provisions of the ACA. In June 2012, we reported[18] that the tax-related provisions established by the ACA affect millions of taxpayers and are key to meeting the primary legislative goal to reform health care. The ACA contains many provisions that are to be implemented over the course of several years, including some that required implementation during the year the legislation was signed into law. Regarding the IRS's planning for the ACA, this audit found that appropriate plans had been developed to implement tax-related provisions of the ACA using well-established methods for implementing tax legislation. The IRS's plans addressed tax forms, instructions, and most affected publications, as well as employee training, outreach and guidance to taxpayers and preparers, computer programming, and data needed for ACA provisions.

The IRS projected its FY 2012 and 2013 ACA staffing needs to be 1,278 Full-Time Equivalents and 859 Full-Time Equivalents, respectively. The IRS has not yet projected staffing needs beyond FY 2013. A lack of documentation to support the staffing requirements needed to implement the ACA precluded the TIGTA from providing an opinion on the adequacy of staffing requests. The IRS did not analyze each provision to determine the amount of staffing necessary to implement the provision. The TIGTA recommended that the IRS perform an analysis to evaluate the resources necessary to efficiently implement the provisions and ensure that this process is documented. The report stated that the IRS plans to complete an evaluation of the major ACA provisions for which implementation has not been completed and evaluate the resources needed for implementation, especially any with specialized skill needs, by the end of FY 2012.

Also in FY 2012, the GAO reported[19] that the IRS had implemented one of its four recommendations from June 2011, to strengthen implementation efforts for the ACA by scheduling the development of performance measures for the IRS ACA program. The GAO's report noted that the IRS had made varying degrees of progress on the other three recommendations: (1) develop program goals and an integrated project plan, (2) develop a cost estimate consistent with GAO's published guidance, and (3) assure that the IRS's risk management plan identifies strategic-level risks and evaluates associated mitigation options.

[18] See Appendix IV, Reference Number 2012-43-064.
[19] GAO, GAO-12-690, *Patient Protection and Affordable Care Act: IRS Managing Implementation Risks, but Its Approach Could Be Refined* (June 2012).

The GAO report concluded that the IRS's revised risk management plan meets three of five criteria for risk management plans, but the plan does not have specific guidance for evaluating and selecting potential risk mitigation options, such as how to (1) identify who conducts and reviews the analysis, (2) determine the availability of resources for a given strategy, and (3) document for future users the rationale behind decisions made.

Further, the GAO reported that the IRS's risk management plan was not used when the IRS's Office of Chief Counsel was responsible for implementing two provisions the GAO reviewed. Although these provisions primarily required legal counsel and guidance, IRS officials said that one of the provisions also affected IRS operations and could have risks that need to be managed. Additionally, the GAO did not find evidence that a risk plan was used to track and mitigate risks when coordinating with partner agencies, such as the Department of Health and Human Services. We agree with the GAO's conclusion that without a system for tracking shared risks, the IRS is more likely to overlook risks or duplicate efforts.

Information Security Background

As our Nation's tax collector and administrator of the Internal Revenue Code, the IRS processed more than 234 million tax returns, of which 143 million came from individuals during FY 2011. Information from these tax returns is converted into electronic format. The IRS maintains 178 computer system applications for use by IRS employees and relies extensively on computerized systems to support its tax administration and core business processes. As such, effective information systems security is essential to ensure that data are 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 faces the daunting task of securing its computer systems against the growing and diverse threats of cyberattacks. As such, the IRS must ensure that its computer systems are effectively secured to protect sensitive financial and taxpayer data. According to the Office of Management and Budget's FY 2011 report to Congress on the implementation of the Federal Information Security Management Act of 2002,[20] the number of cyber incidents affecting Federal Government agencies increased approximately 5 percent in FY 2011, when agencies reported 43,889 cyberattacks to the U.S. Computer Emergency Readiness Team, as presented in Figure 2.

[20] Pub. L. No. 107-347, Title III, 116 Stat. 2899, 2946-2961 (2002) (codified as amended in 44 U.S.C. §§ 3541–3549).

Figure 2: Cyber Incidents Reported to the U.S. Computer Emergency Readiness Team by Federal Agencies in FY 2011

Incident Category	Number of Incidents	Percentage of Total Incidents
Malicious Code	11,626	26.5%
Improper Usage	8,416	19.2%
Unauthorized Access	6,985	15.9%
Scans, Probes, and Attempted Accesses	2,942	6.7%
Denial of Service	30	0.1%
Under Investigation/Other	13,890	31.6%
Total	43,889	100.0%

Source: The Office of Management and Budget's FY 2011 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002.

For FY 2012, we designated "Security for Taxpayer Data and Employees" as the top management challenge for the IRS. This priority designation was given due to the increasing threats, both cyber and physical, against the IRS; the need for the IRS to continue improving its security posture; and the large volumes of data collected, processed, and maintained by the IRS. The IRS is highly visible, with more than 100,000 employees and contractors working in more than 700 facilities. Though animosity toward the IRS is nothing new, the February 2010 aircraft attack on an IRS facility in Austin, Texas, was a stark reminder of the dangers facing IRS employees and highlights a surge in hostility toward the Federal Government. Also, the ongoing public debate regarding the ACA and continued concerns over the country's recovering economy could fuel threats against the Federal Government, including IRS employees, facilities, and systems.

Progress Is Being Made to Improve Information Security and Personnel Safety

The Office of Cybersecurity within the IRS IT organization is responsible for protecting taxpayer information and the IRS's electronic systems, services, and data from internal and external cyber security-related threats by implementing world-class security practices in planning, implementation, risk management, and operations. In addition to providing policy and guidance, the Cybersecurity organization 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 IT Security Program Plan, issued in September 2009. The IT Security

Program Plan is designed to enhance collaboration, provoke thought and comment, and guide all security efforts across the IRS community. In addition, it serves as a roadmap and a basis for benchmarking information security performance toward attaining security objectives. Finally, senior leaders of the IRS will be able to use the IT Security Program Plan as input to their strategic business planning process. This plan is being updated to reflect the current environment and should be completed in September 2012.

During FY 2012, we conducted several audits and found that the IRS is moving toward a more effective information security program.

- During our audit of the February 2010 aircraft attack at the IRS Austin facility, we found the IRS adequately prepared for and took the necessary actions to evacuate and protect IRS employees, secured taxpayer data and Federal Government property, and timely resumed business operations following the incident.[21] The IRS provided extensive personnel services to assess and support affected employee needs, identified temporary office space for the affected employees, awarded several procurements to support the recovery effort in an expedited time period, and provided the furnishings and equipment needed to resume work within 18 calendar days of the incident.
- During an inspection conducted by the TIGTA Office of Inspections and Evaluation on the IRS's contract security guard workforce, we found that the IRS generally has controls in place to ensure these security guards are suitable for employment in the 36 facilities for which it was responsible.[22]
- 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 and the Department of Homeland Security identified 11 information security areas to be evaluated under the Federal Information Security Management Act review. Based on our work during the reporting period July 2010 to June 2011, we determined that 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.[23] Specifically, the IRS met the level of performance for seven program areas: risk management, incident response and reporting, remote access management, continuous monitoring management, contingency planning, contractor systems, and security capital planning. 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 remaining four program areas: configuration management, security training, the process for managing weaknesses, and identity and access management. These results were an improvement

[21] See Appendix IV, Reference Number 2012-10-074.
[22] See Appendix IV, Reference Number 2012-IE-R002.
[23] See Appendix IV, Reference Number 2011-20-116.

from the previous year, when we found that the IRS met an effective level of performance in only three areas: certification and accreditation, incident response and reporting, and remote access management.

- During our audit of incident handling, we found that the Computer Security Incident Response Center was effectively performing its duties and responsibilities to detect, respond, and prevent computer security incidents.[24] We also found that the Center has sufficient tools and training to accomplish its mission.
- During our audit of patch management, we found that the IRS had established policy and guidance for IRS organizations to carry out their respective responsibilities regarding patch management. This policy was consistent with Federal guidance from the National Institute of Standards and Technology, the Department of the Treasury, and industry best practices. In addition, the IRS took steps to automate the installation and monitoring of patching in a large segment of its Windows® environment.
- During our audit of two-factor authentication with Homeland Security Presidential Directive-12 Personal Identity Verification cards, we found that the IRS updated its implementation policies and developed a two-factor authentication system with the required components.[25] In addition, the technical specifications for the acquired products met Federal standards.

Despite this progress, the IRS needs to continue placing emphasis and attention on its information and physical security programs in order to ensure that policies, procedures, and practices adequately address security control weaknesses throughout the organization.

Continued Management Attention Is Needed to Address Weaknesses in Information and Physical Security

Computer security remains as a material weakness

The Federal Managers' Financial Integrity Act of 1982[26] 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 that 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.

[24] See Appendix IV, Reference Number 2012-20-019.
[25] See Appendix IV, Reference Number 2012-20-112.
[26] 31 U.S.C. §§ 1105, 1113, 3512.

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, it has closed or completed all planned corrective actions for eight of the nine components, as shown in Figure 3.

Figure 3: Status of Computer Security Material Weakness Components

Material Weakness Area	Status	Date Closed or to Be Closed
Area 1-1: Network Access Controls	All actions completed.	July 2010
Area 1-2: Application/System Access Controls	All actions completed.	December 2011
Area 1-3: System Software Configuration	All actions completed.	December 2011
Area 1-4: Security Roles and Responsibilities	All actions completed.	March 2009
Area 1-5: Security and System Administration Segregation	Closed.	September 2004
Area 1-6: IT Contingency Planning	All actions completed.	December 2011
Area 1-7: Audit Trails	Open.	January 2014
Area 1-8: Security Training	Closed.	June 2008
Area 1-9: Certification and Accreditation	Closed.	December 2008

Source: The IRS's Computer Security Material Weakness Plan, updated as of December 7, 2011.

Since our last annual assessment report where we cited that the IRS had closed or completed corrective actions for five of the nine areas, the IRS reported that it had completed all corrective actions for three additional areas in December 2011. As early as June 2000, we have performed independent validation assessments over individual areas of the computer security material weakness when requested by the IRS. These audits were specifically conducted to evaluate the effectiveness of actions completed and to provide an opinion on whether the IRS should close or downgrade any areas of the computer security material weakness. The most recent IRS request

came for the IT Contingency Planning area. Accordingly, we completed two audits to assess the effectiveness and completion of the IRS's corrective actions on the IT Contingency Planning area.[27] As a result, we provided verbal concurrence to the IRS that it could either downgrade or close this area, allowing the IRS to make the final determination.

We have not received any other requests to assess the effectiveness of completed corrective actions from the IRS on the Network Access Controls, Application/System Access Controls, or System Software Configurations areas. However, our audits conducted during FY 2012 continued to identify weaknesses related to the computer security material weakness areas. The IRS agreed with the following findings and provided adequate corrective actions to address our findings.

- During our audit of the CADE 2 system database implementation, we found that the IRS did not correct security weaknesses identified through repeated database security vulnerability scans.[28] Specifically, these security weaknesses included privileged users with unauthorized access to tables, packages, and files, which could result in loss of taxpayer data. In addition, configuration weaknesses existed relating to default ports and enabled demonstration tables, which could be exploited because default tables use default account identification names, passwords, and ports.
- During our audit of patch management,[29] we found that the IRS had not yet discovered all the IT assets residing on its network and, therefore, cannot ensure all assets are appropriately patched.[30] We also found that, on several internal management reports, the IRS continues to report missing patches and patches not being timely applied. For example, in March 2012, the IRS's overall patch compliance rate for critical patches averaged 88 percent for all reporting entities. The 12 percent noncompliance rate translated to 23 critical patches not applied to IRS Windows servers, which resulted in 7,329 vulnerabilities remaining on these servers. These vulnerabilities could potentially be exploited to gain unauthorized access to information, disrupt operations, or launch attacks against other systems.
- Also during our audit of patch management, we found that the IRS network contained outdated operating systems, which cannot be patched to correct known security vulnerabilities. For example, we identified 65 obsolete Windows[31] servers on the IRS network. The IRS did not know why these servers were still operational and connected to

[27] See Appendix IV, Reference Number 2012-20-041 and TIGTA, Ref. No. 2011-20-060, *Corrective Actions to Address the Disaster Recovery Material Weakness Are Being Completed* (June 2011).
[28] See Appendix IV, Reference Number 2012-20-109.
[29] Patch management is a component of the Systems Software Configuration area.
[30] See Appendix IV, Reference Number 2012-20-112.
[31] These 65 servers consisted of Windows NT servers (not supported by the Microsoft Corporation since December 31, 2004) and Windows 2000 servers (not supported by the Microsoft Corporation since July 13, 2010).

its network. Outdated operating systems are no longer supported by the vendor, which means new vulnerabilities cannot be corrected and can be exploited.

- During our audit of IRS audit trails to detect unauthorized access by IRS employees,[32] we found that the IRS needs to ensure audit trails effectively support unauthorized access investigations in order for the IRS to make further progress in addressing and resolving the audit trail material weakness.[33] As of March 2012, the audit trail repository system where audit trails are maintained for monitoring efforts contained audit trails for only 20 systems. The IRS estimated that 339 systems or subsystems could potentially be required to be monitored.

In addition, from April 2011 to March 2012, the GAO assessed whether controls over key financial and tax processing systems were effective in ensuring the confidentiality, integrity, and availability of financial and sensitive taxpayer information in conjunction with its audits of the IRS's FYs 2010 and 2011 financial statements. The GAO found that the IRS implemented numerous controls and procedures intended to protect key financial and tax-processing systems; however, control weaknesses in these systems continue to jeopardize the security of financial and sensitive taxpayer information processed by the IRS's systems. Specifically, the IRS continues to face challenges in controlling access to its information resources. For example, it had not always (1) implemented controls for identifying and authenticating users, such as requiring users to set new passwords after a prescribed time period; (2) appropriately restricted access to certain servers; (3) ensured that sensitive data were encrypted when transmitted; (4) audited and monitored systems to ensure that unauthorized activities would be detected; or (5) ensured management validation of access to restricted areas. In addition, unpatched and outdated software exposed the IRS to known vulnerabilities, and the agency had not enforced backup procedures for a key system.

Considered collectively, these deficiencies, both new and unresolved from previous GAO audits, along with a lack of fully effective compensating and mitigating controls, impair the IRS's ability to ensure that its financial and taxpayer information is secure from internal threats. This reduces the IRS's assurance that its financial statements and other financial information are fairly presented or reliable and that sensitive IRS and taxpayer information is being sufficiently safeguarded from unauthorized disclosure or modification. These deficiencies are the basis of the GAO's determination that the IRS had a material weakness in internal controls over financial reporting related to information security in FY 2011.

[32] Internal Revenue Code Section 6103 and the Taxpayer Browsing Protection Act of 1997 (26 U.S.C. §§ 7213, 7213A, and 7431) require the IRS to detect and monitor unauthorized access and disclosure of taxpayer data. The willful unauthorized access or inspection of taxpayer records is a criminal offense.
[33] See Appendix IV, Reference Number 2012-20-099.

Other security weaknesses adversely affect the IRS's ability to achieve effective information and physical security programs

In addition, we identified security weakness areas from across several audits during our reporting period.

- Physical security.
  - Because of the Austin aircraft attack, the IRS contracted for the completion of in-depth physical security reviews of IRS facilities across the country to determine how to improve its current security posture. During our audit of this contract, we found that IRS employees did not properly administer the contract in compliance with acquisition regulations and directed the contractor to perform services that were lesser in scope than required by the contract.[34] As a result, the contractor did not perform an in-depth, independent assessment regarding the security posture of the IRS's facilities. The noncompliance of contract deliverables could potentially impact the IRS's ability to make informed decisions regarding its physical security and the need for additional security enhancements.
- Remediation of security weaknesses.
  - The security weaknesses previously discussed on unauthorized access to privileged user accounts from our review of the CADE 2 system database implementation were the result of an ineffective process for remediating identified security weaknesses during systems development. Database vulnerability scans in March 2012 identified 67 weaknesses, of which 49 were deemed critical and 18 were deemed major. A comparison to a similar scan performed in December 2011 showed that the weaknesses were repeat findings.
  - The security weakness previously discussed on missing critical patches from our review of patch management were partly caused by insufficient monitoring processes to ensure vulnerabilities resulting from unpatched systems were successfully and timely remediated. Monitoring servers and workstations were performed manually with self-reported results or conducted by an automated solution that had not been properly implemented or was not working as intended.
- Lack of oversight or functional coordination on security-related issues.
  - During an inspection conducted by the TIGTA Office of Inspections and Evaluation on the IRS's contract security guard workforce, we found that the IRS had erroneously allowed 17 contract security guards to continue to work at an IRS facility after their access authorization had expired.

[34] See Appendix IV, Reference Number 2012-10-075.

- During our audit of the CADE 2 system database implementation, we found that the IRS hired two contractors to conduct source code reviews of the CADE 2 system database; the contractors identified one high-risk and several moderate- and low-risk weaknesses in October 2011. These weaknesses included Structured Query Language injection, insufficient password management, incorrect logical operators, and insufficient input validation. The CADE 2 Governance Board chose not to correct these weaknesses, accepting the risks because the code was intended to be used only once. However, we found the unsecure code was used multiple times in testing and to initialize the production database in March 2012, and it will be used to initialize the database in the summer of 2012. These weaknesses could cause a loss of data and performance problems.
- During our audit of incident handling, we found that 34 percent of servers within the IRS network did not have host-based intrusion detection software installed.[35] Host-based intrusion detection software allows the Computer Security Incident Response Center to monitor and analyze network traffic for the purpose of detecting suspicious activities. A lack of coordination between the Center and systems administrators, who are responsible for installing the software, contributed to the significant number of servers without this detection capability.
- During our review of two-factor authentication with Homeland Security Presidential Directive-12 Personal Identity Verification cards (referred to as SmartID cards by the IRS), we found that the project encountered significant delays, putting the IRS 22 months behind its original planned completion date for implementing the new two-factor authentication system.[36] We also believe this project will be further delayed due to inadequate progress being made on mandating the use of SmartID cards, implementing two-factor authentication for administrators, enabling the use of SmartID cards for authentication to applications, and configuring remote access capabilities to use SmartID cards. We also found that required testing, including security testing, was not conducted and that key enterprise lifecycle artifacts and processes were not completed. Many of these weaknesses were attributed to a lack of a project manager with the requisite training and experience to manage and oversee the project.

Until the IRS 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 and employee safety at risk.

[35] See Appendix IV, Reference Number 2012-20-019.
[36] See Appendix IV, Reference Number 2012-20-115.

Information Technology Operations Background

The IRS IT organization plays an important role in helping the IRS meet its tax administration responsibilities each year. It is not only responsible for the efficient and secure processing and transfer of taxpayer data, but it also supports the needs of 100,000 employees who rely on equipment and system availability. The IRS needs to ensure that it leverages viable technological advances as it improves its overall operational environment.

According to the Draft IRS IT Business Plan FYs 2011–2013, the IRS IT organization's vision is to become a world-class provider of IT services by focusing on people, processes, and technology. Because these components are interlinked, it is imperative to create an alignment between each of these three areas. Focusing on developing employees is the most important activity. Then, focusing on process functions allows the IT organization to focus on activities that add customer value while increasing operational efficiency and decreasing cost. Finally, the identification and implementation of appropriate technology solutions provides a path to organizational success.

Information Technology Operational Efficiency Continues to Improve, but Additional Improvements Are Needed

During FY 2012, we conducted several audits of IT operations and found opportunities for the IRS to improve operational efficiency and effectiveness.

During our audit to evaluate the effectiveness and efficiency of the IRS's efforts to consolidate and virtualize its servers, we found that by the end of FY 2011, the Server Consolidation and Virtualization Project team had succeeded in establishing a virtual Wintel server environment with approximately 1,800 virtual servers running on 234 physical host servers at 13 data center locations (nine campuses, three computing centers, and the New Carrollton Federal Building). The goals of the project were successfully achieved on time and within budget.[37] Reducing the number of physical servers has resulted in significant cost savings, associated with lower electrical output for fewer servers, and hardware savings over a one-for-one server replacement. As of the end of FY 2011, the IRS estimated that server virtualization had saved approximately $10.2 million in equipment costs. The IRS also expects to save approximately $1.3 million annually in decreased electrical costs beginning in FY 2013. The virtualized servers help lower operational costs through standardization, making it easier to load or remove a server from the operating environment. Other benefits of virtualization technology include decreased server hardware downtime and automatic load balancing.[38]

[37] See Appendix IV, Reference Number 2012-20-029.
[38] Automatic load balancing refers to the even distribution of processing across available resources such as servers in a network.

However, the Server Consolidation and Virtualization Project team did not include Wintel servers in IRS field offices outside of the 13 targeted locations. IRS management estimates approximately 650 of 1,000 Wintel servers in its field locations can be decommissioned and added to the virtual server environment. By virtualizing the remote servers, IRS management estimates it could realize an additional savings of approximately $7.73 million ($7.26 million in equipment savings and $0.47 million in electrical savings over five years).

During our audit to evaluate the effectiveness and efficiency of the new business processes, the implementation of personnel placement, and mitigations associated with the reorganization of the EUES organization, we found that EUES organization management should introduce measures that will help assess the cost effectiveness of the Customer Service Support Centers.[39] Also, EUES organization management should mandate use of the password management tool. In FY 2010, the Service Desk performed 122,431 password resets, and in FY 2011, it performed 130,806 password resets, with 12,000 of these occurring during a one-month period. These high password reset rates occurred because management had not mandated the use of the password management tool. Mandating the use of this tool will allow the IRS to achieve the full benefits from the tool while freeing up Service Desk employees to focus on resolving other complex issues and increasing its first contact resolution rate.

The Information Technology Organization Is Effectively Working Human Capital Issues, but Additional Improvements Are Needed

The Human Capital Assessment and Accountability Framework identify five human capital systems that together provide a consistent, comprehensive representation of human capital management for the Federal Government. The Human Capital Assessment and Accountability Framework links human capital management to the merit system principles and other civil service laws, rules, and regulations. The establishment of the Human Capital Assessment and Accountability Framework fulfills the Office of Personnel Management Chief Human Capital Officers Act of 2002[40] to design systems and set standards, including appropriate metrics, for assessing the management of human capital by Federal agencies.

Workforce planning is a systematic process for identifying the human resources required to meet an agency's mission and goals and developing strategies to meet those requirements. According to the Office of Personnel Management,[41] an effective workforce plan includes identifying the human capital required to meet organizational goals, conducting analysis to identify competency gaps, developing strategies to address human capital needs and close competency gaps, and ensuring the organization is appropriately structured. An agency should approach workforce

[39] See Appendix IV, Reference Number 2012-20-086.
[40] 5 U.S.C 1103 (c) and implemented under subpart b of 5 CFR part 250.
[41] The Office of Personnel Management, *The Office of Personnel Management Human Capital Assessment and Accountability Framework Resource Center – Workforce Planning (Strategic Alignment System)* (Sept. 2005).

planning strategically and in an explicit, documented manner. The workforce plan should link directly to the agency's strategic and annual performance plans and be used to make decisions about structuring and deploying the workforce. One key element of workforce planning requires a workload analysis to determine the size of the workforce needed to meet organizational goals and to identify gaps between current and future workforce needs before the new budget execution cycle.

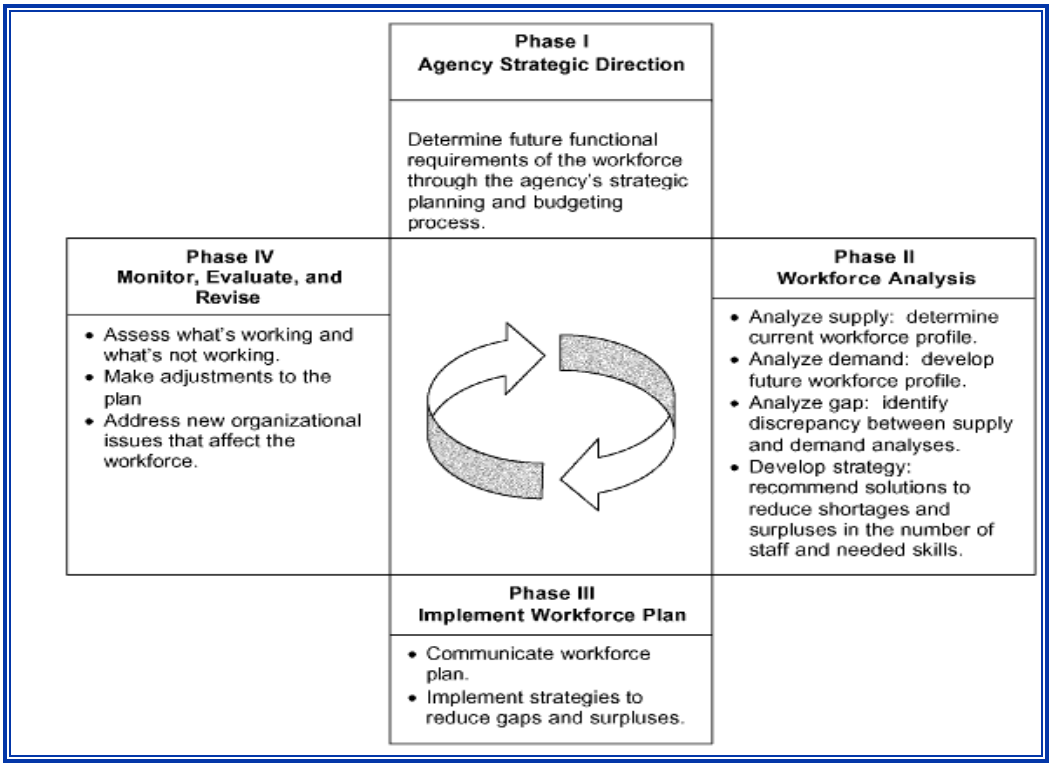
The IRS IT organization is striving to achieve the objective to "make the IRS the best place to work in government," but managing the drivers of change becomes a workforce planning challenge due to the following needed factors:

- Ability to compete as an employer in the external marketplace, as well as improve upon hiring goals and processes.
- Continued improvement in tracking and forecasting workforce needs and changes.
- Continued improvement of employee engagement and identifying and developing its future leaders of tomorrow.
- Ability to measure and respond to the results of its human resource plans and processes.[42]

The Internal Revenue Manual provides guidance and standards for establishing workforce planning. Similar to the Office of Personnel Management model, Figure 5 shows four phases of the IRS Strategic Workforce Planning model.

[42] See Appendix IV, Reference Number 2012-20-107.

Figure 5: IRS Strategic Workforce Planning Model for Human Resources Management



Source: Internal Revenue Manual Exhibit 6.251.1-3, dated July 2003.

During our audit to evaluate the effectiveness and efficiency of the new business processes, the implementation of personnel placement, and mitigations associated with the reorganization of the EUES organization, we found that impacted employees were provided mitigation strategies during placement into the reorganized EUES organization. Some of the mitigations or placements offered included realignment, voluntary retirement/separation for those deemed eligible, preference placement, voluntary or involuntary reassignment, and competitive placement. The EUES organization established a baseline of 1,292 employees, of which approximately 1,100 were bargaining unit employees.[43] As of December 2011, the EUES organization placed 1,211 of its employees into the new structure.

In addition, placed employees received training to handle new roles and responsibilities. The EUES organization management developed a comprehensive training curriculum for each position within the various EUES functions. The curriculum detailed the training classes needed to successfully perform in a given job. An analysis of training records obtained from EUES organization management showed Service Desk and deskside employees received training within

[43] The baseline was established in October 2009.

the parameters defined by the Memorandum of Understanding and National Treasury Employees Union agreements to prepare them for their jobs.

We also interviewed six Service Desk employees regarding special training they might have received to prepare them for providing the first-line of customer service. We were informed that in addition to completing a two-week training course about the Service Desk, each was assigned an on-the-job training instructor to provide further assistance.

During our audit to evaluate the IRS IT organization's workforce planning efforts to ensure that it had the human capital needed to deliver IT services and solutions that drive effective tax administration, we found that the IT organization had conducted an extensive study to determine if any human resource contention risks existed related to its staffing demand forecasts and developed mitigation strategies for areas of risk as appropriate. Although the IRS IT organization had a process for identifying its resource needs and gaps for completing its priority work, the process primarily relied on management's knowledge and judgment about each individual's skills and did not consider resource needs for other mission-related work. While there are some automated personnel systems that provide IRS IT organization management with information about its employees, *e.g.*, certifications obtained and educational holdings, there is not a system within the IRS IT organization that provides information about skills and competencies associated with the various occupations. Without a competency database, IRS IT organization management cannot efficiently and effectively manage the skills of the workforce.

Appendix I

Detailed Objective, Scope, and Methodology

The IRS Restructuring and Reform Act of 1998,[1] in part, states that the TIGTA shall annually perform an evaluation of the adequacy and security of the technology of the IRS. To meet this objective, the audit considered results from internal and external reports from August 1, 2011, through September 30, 2012, focusing on key programs and initiatives led by the CTO. Our subobjectives were to:

I. Compile IRS IT Program-related audit findings and recommendations from TIGTA reports and identify high-risk IT management issues affecting IRS efforts to achieve its program goals and objectives.

II. Consider pertinent status information from other internal and external IRS oversight organizations, including published reports.

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. We did not evaluate internal controls as part of this review because doing so was not necessary to satisfy our review objective.

[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.).

Appendix II

Major Contributors to This Report

Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)
Gwendolyn McGowan, Director
Kent Sagara, Director
Danny Verneuille, Director
Carol Taylor, Audit Manager
Ryan Perry, Lead Auditor
Louis Lee, Senior Auditor
Mike Mohrman, Information Technology Specialist

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Assistant Deputy Commissioner for Operations Support OS
Chief, Agency-Wide Shared Services OS:A
Deputy Chief Information Officer for Operations OS:CTO
Deputy Chief Information Officer for Strategy/Information Technology OS:CTO
Deputy Commissioner, Services and Operations SE:W
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 Networks OS:CTO:UNS
Associate Chief Information Officer, Enterprise Operations OS:CTO:EO
Associate Chief Information Officer, Enterprise Services OS:CTO:ES
Associate Chief Information Officer, Information Technology – Program Management Office OS:CTO:MP
Associate Chief Information Officer, Strategy and Planning OS:CTO:SP
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 Liaison: Director, Risk Management Division OS:CTO:SP:RM

Appendix IV

List of Treasury Inspector General for Tax Administration Reports Reviewed

No.	Report Reference or (Audit) Number	Report Title	Report Issuance Date
1	2011-20-116	*Treasury Inspector General for Tax Administration – Federal Information Security Management Act Report for Fiscal Year 2011*	September 20, 2011
2	2011-10-098	*The Internal Revenue Service Adequately Prepared for and Responded to the Austin Incident*	September 21, 2011
3	2011-20-111	*Continued Centralization of the Windows Environment Would Improve Administration and Security Efficiencies*	September 23, 2011
4	2012-IE-R002	*Internal Revenue Service Contract Security Guard Workforce Inspection*	January 10, 2012
5	2012-20-019	*The Computer Security Incident Response Center Is Effectively Performing Most of Its Responsibilities, but Further Improvements Are Needed*	March 12, 2012
6	2012-20-029	*Virtual Server Technology Has Been Successfully Implemented, but Additional Actions Are Needed to Further Reduce the Number of Servers and Increase Savings*	March 30, 2012
7	2012-20-041	*Disaster Recovery Testing Is Being Adequately Performed, but Problem Reporting and Tracking Can Be Improved*	May 3, 2012

No.	Report Reference or (Audit) Number	Report Title	Report Issuance Date
8	2012-20-051	*Customer Account Data Engine 2 Performance and Capacity Is Sufficient, but Actions Are Needed to Improve Testing*	May 16, 2012
9	2012-43-064	*Affordable Care Act: Planning Efforts for the Tax Provisions of the Patient Protection and Affordable Care Act Appear Adequate; However, the Resource Estimation Process Needs Improvement*	June 14, 2012
10	2012-10-074	*Accounting for the Austin Incident*	July 10, 2012
11	2012-10-075	*An Independent Risk Assessment of Facility Physical Security Was Not Performed in Compliance With Contract Requirements*	July 25, 2012
12	2012-20-086	*The End-User Equipment and Services Organization Successfully Planned Its Reorganization; However, Program Measures and Efficiencies Can Be Improved*	August 14, 2012
13	2012-40-116	*While Use of the Modernized e-File System for Individual Tax Returns Has Increased, the Legacy e-File System Is Still Needed As a Backup*	September 19, 2012
14	2012-20-099	*Audit Trails Did Not Comply With Standards or Fully Support Investigations of Unauthorized Disclosure of Taxpayer Data*	September 20, 2012
15	2012-20-107	*The Information Technology Organization Needs to Implement a Competency Database to Efficiently Manage Its Workforce*	September 21, 2012
16	2012-20-112	*An Enterprise Approach Is Needed to Address the Security Risk of Unpatched Computers*	September 25, 2012

No.	Report Reference or (Audit) Number	Report Title	Report Issuance Date
17	2012-20-122	*Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements*	September 28, 2012
18	2012-20-121	*Despite Steps Taken to Increase Electronic Returns, Unresolved Modernized e-File System Risks Will Delay the Retirement of the Legacy e-File System and Implementation of Business Forms*	September 27, 2012
19	2012-20-109	*The Customer Account Data Engine 2 Database Was Initialized; However, Database and Security Risks Remain, and Initial Timeframes to Provide Data to Three Downstream Systems May Not Be Met*	September 27, 2012
20	2012-20-115	*Using SmartID Cards to Access Computer Systems Is Taking Longer Than Expected*	September 28, 2012

Appendix V

Number of Internal Revenue Service Information Technology Employees

IRS Information Technology	Number of Employees June 30, 2012
Applications Development	2,321
Enterprise Services	280
Strategy and Planning	322
User and Network Services	1,692
Enterprise Operations	1,717
Cybersecurity	382
Affordable Care Act Program Management Office	288
Management Services	146
Customer Account Data Engine Program Management Office	70
Chief Technology Officer Office	4
Deputy Chief Information Officer for Strategy and Modernization	4
Deputy Chief Information Officer for Operations	2
TOTAL	**7,228**

Source: Treasury Integrated Management Information System as of June 30, 2012.

Appendix VI

Glossary of Terms

Term	Definition
Audit Trails	A record of events occurring on a computer from system and application processes as well as user activity.
Best Practice	A technique or methodology that, through experience and research, has proven to lead to a desired result.
Business Master File	The database on which the IRS stores business taxpayers' data.
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.
Campus	The data processing arm of the IRS. The campuses process paper and electronic submissions, correct errors, and forward data to the Computer Centers for analysis and posting to taxpayer accounts.
Certification and Accreditation	A process to provide assurance that adequate security controls are in place over computer systems.
Competency	An observable, measurable skill set of skills, knowledge, abilities, behaviors, and other characteristics an individual needs to successfully perform work roles or occupational functions. Competencies are typically required at different levels of proficiency depending on the specific work role or occupational function. Competencies can help ensure individual and team performance aligns with the organization's mission and strategic direction.
Computing Centers	Support tax processing and information management through a data processing and telecommunications infrastructure.
Configuration Management	A collection of activities focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configurations of those products and systems.

Term	Definition
Continuous Monitoring	Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.
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.
Default	Controls or settings of computer hardware or software as preset by its manufacturer. Some types of default settings may be altered or customized by the user.
Denial of Service	The prevention of authorized access to resources or the delaying of time-critical operations.
Earned Value Management	A structured process used to manage major investments, which integrates the scope of work with schedule and cost elements for better planning and control.
Earned Value Management Data	Quarterly data that shall be provided to the Department of the Treasury. This data must be entered into the Department of the Treasury portfolio management tool and obtained from the Bureau's Earned Value Management System to fulfill Department of the Treasury and Office of Management and Budget reporting requirements.
Earned Value Management System	A system that the Office of Management and Budget requires Federal agencies use to manage all major IT investments with development/modernization/enhancements activities.
Federal Information Security Management Act of 2002	Legislation that 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.

Term	Definition
Homeland Security Presidential Directive-12 (HSPD) Personal Identity Verification Card	This directive established a new standard for issuing and maintaining identification badges (also known as Personal Identity Verification cards) for Federal employees and contractors entering Government facilities and accessing computer systems.
Human Capital	Defined by the National Academy of Public Administration as the "identification of competencies and skills needed to realize an organization's operating goals." According to the GAO, acquiring and developing staffs whose size and skills meet agency needs is one of the most pervasive challenges facing the Federal Government.
Individual Master File	The IRS database on which the IRS stores individual taxpayers' data.
Information Reporting and Document Matching	The IRS established this program to create the infrastructure needed to implement two pieces of tax-gap legislation related to third-party reporting.
Integrated Data Retrieval System	Manages data that was extracted from the Corporate Account Data Stores (Business Master File, Employee Plans Master File, Individual Master File, and CADE) allowing IRS employees to take specific actions on taxpayer account issues, track status, and post transaction updates to the Master Files. It provides for systemic review of case status and notice issuance based on case criteria, alleviating staffing needs and providing consistency in case control.
JAVA	A general purpose, concurrent, class-based, object-oriented language that is specifically designed to have as few implementation dependencies as possible.
Malicious Code	The term used to describe any code in any part of a software system or script that is intended to cause undesired effects, security breaches, or damage to a system. Malicious code describes a broad category of system security terms that includes attack scripts, viruses, worms, Trojan horses, backdoors, and malicious active content.

Term	Definition
Material Weakness	Office of Management and Budget Circular A-123, *Management's Responsibility for Internal Control*, 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.
Mitigation Strategies	Strategies used to avoid or lessen the number or severity of involuntary personnel actions that result from an organization change, *e.g.*, Voluntary Early Retirement Authority, Voluntary Separation Incentive Payment, Job Swaps, Grade and Pay Retention.
Modernized e-File (MeF)	The MeF project develops a modernized, web-based platform for filing approximately 330 IRS forms electronically, beginning with the Form 1120, *U.S. Corporation Income Tax Return,* Form 1120S, *U.S. Income Tax Return for an S Corporation*, and Form 990, *Return of Organization Exempt From Income Tax*. The project serves to streamline filing processes and reduce the costs associated with a paper-based process.
Patch Management	The process by which an organization installs patches, which are fixes or updates to computer programs, operating systems, or applications.
Release	A specific edition of software.
Resource Contention	Occurs when multiple projects have the same skill-set needs, but there are not enough resources available to fill the total skill-set needs.
Structured Query Language (SQL) Injection	A type of attack where a malicious entity sends specially crafted input to the content generator. The input includes a specific SQL command string that, when submitted unfiltered to a SQL database server, potentially returns to the attacker any or all of the information stored in the database. SQL injections and other attacks are used to execute commands or gain unauthorized access to the Web server or a backend database server.
Taxpayer Information File	A file containing entity and tax data processed at a given service center for all Taxpayer Identification Numbers.

Term	Definition
Virtual Server	A virtual server is not a physical machine. It co-resides and shares computer resources with other virtual servers on a physical computer or host.
Voluntary Early Retirement Authority	An opportunity to retire in advance of meeting the age and/or service requirements normally needed for retirement.
Voluntary Separation Incentive Payment	Commonly referred to as buyouts. Lump-sum payments of up to $25,000 paid to specifically impacted employees to enhance resignation or retirement. Buyouts are targeted at employees in specific grades, series, and locations and are used to help avoid Reductions in Force and minimize involuntary separations. Agencies, including the IRS, must obtain authority to offer buyouts to their employees from the Office of Personnel Management.
Wintel Server	A server running a Microsoft Windows operating system with an Intel microprocessor.
Workforce Planning	A process whereby a strategic plan is developed which sets the organization's objectives for competency development and workforce activities. These objectives are supported by workforce allocation with each organizational unit to satisfy both unit needs and strategic objectives. The workforce planning process fundamentally involves identifying the gap between the existing workforce supply and the future workforce competency needs and position requirements based on projected workload and strategic objectives. The plan may also enumerate or recommend closing gap strategies and or options for the Senior Leadership Team.