Continued Centralization of the Windows Environment Would Improve Administration and Security Efficiencies

September 23, 2011

Reference Number: 2011-20-111

Phone Number | 202-622-6500
Email Address | TIGTACommunications@tigta.treas.gov
Web Site | http://www.tigta.gov

CONTINUED CENTRALIZATION OF THE WINDOWS ENVIRONMENT WOULD IMPROVE ADMINISTRATION AND SECURITY EFFICIENCIES

Highlights

Final Report issued on September 23, 2011

Highlights of Reference Number: 2011-20-111 to the Internal Revenue Service Chief Technology Officer.

IMPACT ON TAXPAYERS

The Internal Revenue Service (IRS) operates a large computer network that includes about 6,000 servers and 110,000 workstations using Windows operating systems provided by the Microsoft Corporation. Proper implementation of Microsoft Corporation Windows technology simplifies system administration and provides methods to strengthen and consistently secure computer systems. When IRS operations run efficiently and securely, taxpayer dollars and data are preserved and protected.

WHY TIGTA DID THE AUDIT

This audit is included in our Fiscal Year 2011 Annual Audit Plan and addresses the major management challenge of Security. The overall objective of this review was to determine whether the IRS has structured its Windows environment to provide efficient and secure management of Windows servers.

WHAT TIGTA FOUND

The IRS has not taken actions to continue enforcing the centralization of its Windows environment, which would simplify system administration and achieve consistent identity and authentication management that is required by Federal regulations and IRS enterprise architecture security principles. TIGTA found three organizations that maintained groups of Windows servers outside of the main centralized group of Windows servers. The IRS spent $1.2 million in contract fees to maintain obsolete computer equipment in one of these groups, rather than spending those funds to resolve the vulnerability.

In addition, the IRS did not ensure that all Windows computers connected to its network were authorized and compliant with security policy, putting the IRS at risk of security breaches. While the IRS had created standards to prevent unauthorized computers from being connected to the network, it had not established a central controlling authority to enforce compliance with its policy.

WHAT TIGTA RECOMMENDED

The Chief Technology Officer should ensure that: 1) an enterprise-wide governing body is established to enforce Windows server group design criteria and ensure unauthorized Windows server groups are not created; 2) planned shutdown of the noncentralized groups of Windows servers is continued or feasibility studies to collapse noncentralized Windows server groups are completed; 3) standards to prevent computers from being connected to the network without proper authorization and required compliance documentation are implemented enterprise-wide; and 4) network scanning tools are utilized to locate unauthorized computers on the IRS network, and adequate procedures are developed and implemented to ensure they are removed.

In its response to the report, the IRS agreed with TIGTA's recommendations and plans to take appropriate corrective actions. However, the IRS disagreed with TIGTA's $1.2 million outcome measure related to the maintenance of obsolete computer equipment. TIGTA maintains the appropriateness of the measure.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

September 23, 2011

MEMORANDUM FOR CHIEF TECHNOLOGY OFFICER

Michael R. Phillips

FROM: Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Continued Centralization of the Windows Environment Would Improve Administration and Security Efficiencies (Audit # 201120010)

This report presents the results of our review to determine whether the Internal Revenue Service (IRS) has structured its Windows environment to provide efficient and secure management of Windows servers. This audit is included in the Treasury Inspector General for Tax Administration Fiscal Year 2011 Annual Audit Plan and addresses the major management challenge of Security.

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

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

Table of Contents

Abbreviations

BSM	Business Systems Modernization
HSPD-12	Homeland Security Presidential Directive-12
IFS	Integrated Financial System
IRS	Internal Revenue Service
ISRP	Integrated Submission and Remittance Processing
MITS	Modernization and Information Technology Services
SAP	Systems, Applications, and Products
SOI	Statistics of Income

Background

The Internal Revenue Service (IRS) operates a large computer network that includes about 6,000 servers[1] and 110,000 workstations using Windows operating systems provided by the Microsoft Corporation. During Fiscal Year 2005, the IRS implemented Active Directory, a Microsoft Corporation software system for administering and securing computer networks. Active Directory manages the identities and relationships of computing resources that comprise a network. It enables administrators to assign enterprise-wide policies, deploy programs to many computers, and apply critical updates to an entire organization simultaneously from a central, organized, accessible database. It simplifies system administration and provides methods to strengthen and consistently secure computer systems. The benefits of Active Directory's centralized management of computers and users include:

Proper implementation of Active Directory technology simplifies system administration and provides methods to strengthen and consistently secure computer systems.

- Central location for network administration and security.
- The ability to scale up or down easily.
- Synchronization of directory updates across servers.
- The ability to design and deploy enterprise monitoring tools and security solutions.
- Centralized and consistent identity and authentication management.

The IRS's previous network operating system was divided into obsolete and inefficient boundaries, expensive to manage, and difficult to consistently secure. Active Directory supports a centralized approach to system administration that enforces software and security policies across the enterprise.

A forest is the outermost design element or boundary in an Active Directory implementation. As a general rule, best practices dictate that the use of multiple forests for a single application or business process should be avoided. Ideally, there should be only one forest in an organization for maximum administration, cost, and security efficiencies. Because each forest is administered separately, adding additional forests increases an organization's management overhead.

[1] Servers are computers that carry out specific functions. For example, file servers store files, print servers manage printers, and network servers manage network traffic.

A domain is an administrative partition within a forest to manage objects, such as users, groups, and computers. The domain supports a number of core functions related to administration, such as authentication and configuration management. Best practices dictate that the number of domains created within a forest should also be minimized in order to minimize administrative costs. Each additional domain in a forest increases management overhead, requires additional computer hardware, and must have configuration and security policies applied separately.

Domains are further subdivided into organizational units, which are used to uniformly manage administrative groupings of users, groups, and computers. Security settings are consistently applied to all the computers in an organizational unit by linking the appropriate group policy. Linking group policy to organizational units provides a centralized means to control and enforce configuration and security policies. Any computer subsequently added to the organizational unit would automatically receive the appropriate security settings.

In Fiscal Year 2006, the Treasury Inspector General for Tax Administration conducted an audit[2] on the IRS's progress to establish Active Directory enterprise-wide in accordance with industry best practices. The IRS Active Directory Team established the IRS main production forest (called the DS Domain) and intended that it would serve as the shared resource for centralized administration and access control across the IRS enterprise. The Modernization and Information Technology Services (MITS) Enterprise Operations organization maintains the IRS main production forest.

The IRS Active Directory Team also created a forest design policy which stated that application-specific or group-specific Active Directory forests would not be necessary or desirable as a rule. However, the policy allowed IRS entities that could not delegate enterprise administrative rights for reasons of security (e.g., entities that maintain law enforcement information) to create their own forests rather than participate in the IRS main production forest. Although the MITS organization never finalized this design policy, IRS policy states that the MITS organization is responsible for establishing and managing the IRS Active Directory network topology.[3]

The vast majority of IRS Windows computers and users are included in the IRS main production forest, which contains a root domain, a test domain, and one large production domain. At the time of our prior review, additional forests had been created for two IRS organizations (the Office of Chief Counsel and Criminal Investigation) that needed greater security for protection of law enforcement information and justified the need for separate forests. A forest called Business Systems Modernization (BSM) was also created for the Integrated Financial System

[2] *The Enterprise-Wide Implementation of Active Directory Needs Increased Oversight* (Reference Number 2006-20-080, dated May 9, 2006).
[3] Network topology is the layout pattern of interconnections of the various elements of a computer network.

(IFS)[4] because it was implemented before the IRS was ready to deploy the main production forest. However, this system did not meet the IRS's criteria for establishing a separate forest; therefore, the IRS had agreed that consideration should be given to bringing it into the IRS's main production forest to achieve maximum efficiencies and security of IRS operations. However, the BSM forest remains as a separate forest to date.

We reported that the IRS should enforce its Active Directory design standards because adding unnecessary separate forests would increase the cost of implementing and maintaining Active Directory and would make maintaining consistent security controls more difficult. Because the new Active Directory Team and leadership were already aware of these implementation issues, we made no recommendations to address the multiple forest issue.

This review was performed at the Detroit Computing Center in Detroit, Michigan; the Fresno Campus[5] in Fresno, California; the Ogden Campus in Ogden, Utah; the Office of Chief Counsel in San Francisco, California; Criminal Investigation in Florence, Kentucky; and the Enterprise Operations organization in Oakland, California, during the period October 2010 through July 2011. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings 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.

[4] The IFS manages the IRS's $11.4 billion operating budget for administering tax payments, collection, and enforcing tax laws.
[5] The data processing arm of the IRS. The campuses process paper and electronic submissions, correct errors, and forward data to the Computing Centers for analysis and posting to taxpayer accounts.

Results of Review

Actions Are Needed to Allow Active Directory to Simplify System Administration

Despite IRS plans to establish one main shared Windows administrative boundary (i.e., forest) to achieve maximum administration, cost, and security efficiencies, Figure 1 shows the IRS organizations, in addition to Enterprise Operations organization, that have established their own forests for managing their Windows servers. Based on our review of IRS policy, industry best practices for Windows environments, and the reasons for which the various forests were established, we believe five of the eight IRS organizations were justified in establishing separate forests.

Figure 1: IRS Business Organizations That Maintain Active Directory Forests

IRS Business Organization	Number of Forests	Number of Windows Servers	Justified as Separate Forest?
Enterprise Operations	1	4,042	Yes; IRS main production forest
IRS Development Forest	1	171	Yes; isolated forest for test and development purposes
Chief Counsel	2	449	Yes; contains law enforcement data
Criminal Investigation	1	615	Yes; contains law enforcement data
Computer Security Incident Response Center	1	76	Yes; contains tools for scanning and managing vulnerabilities that require isolation
BSM	1	24	No
Statistics of Income (SOI)	4	92	No
Integrated Submission and Remittance Processing (ISRP)	9	210	No
TOTAL		5,679	

Source: IRS organizations provided the numbers of Windows servers in their inventories during the course of our review. We provided the conclusion on whether the various forests were justified, based on our audit work.

Three IRS organizations, BSM, SOI, and ISRP, created 14 forests that did not meet MITS organization criteria or industry best practices for establishing a separate forest and should be merged into the IRS's main production forest to achieve maximum administration efficiencies and security of IRS operations.

In addition, users in the BSM, SOI, and ISRP organizations' forests generally have multiple logon accounts, which impede the IRS from establishing centralized and consistent identity and authentication management in adherence with Homeland Security Presidential Directive 12 (HSPD-12) smart card[6] logon requirements and IRS enterprise architecture security principles. HSPD-12, signed by the President on August 27, 2004, established the requirements for a common identification standard for identity credentials issued by Federal Government departments and agencies to Federal employees and contractors for gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems. IRS enterprise architecture security principles call for the identities and authenticators of as many users as possible to be stored and managed in a centralized database. Therefore, solutions should be found to consolidate the BSM, SOI, and ISRP organizations' forests into the IRS main production forest and require users to authenticate through it. The IRS main production forest is already enabled for smart card logon, a Federal requirement that all of the IRS must work towards.

Having the least number of forests in the IRS environment would achieve the maximum amount of administration efficiencies and would result in costs savings by eliminating administrative responsibilities from the 14 forests. The IRS would also incur significant transition and implementation costs as the IRS attempts to get to this target state. As a result, we were unable to specifically measure the savings expected to be achieved in the long run, since costs to collapse existing forests may exceed savings in the short term, pushing out the return on investment.

The BSM organization forest is obsolete and should be removed

The IRS contracted with the IBM Corporation to setup the BSM organization forest as a means to authenticate users to the IFS application when it went into production in November 2004, before the IRS main production forest was implemented. However, once the IRS main production forest was implemented, efficiencies could have been achieved if BSM organization servers were upgraded to Windows 2003, allowing the BSM organization forest to be merged into the IRS main production domain. Currently, the BSM organization forest consists of primarily legacy Windows 2000 servers, which are outdated and no longer supported by the Microsoft Corporation. Patches are no longer issued for these servers, which remain a high security risk.

In addition, the current method used to authenticate users to the IFS has an access vulnerability that allows users and system administrators to remotely logon using an unsecured alternative path. This remote logon access, intended to be used only in emergencies by system administrators when no other access to the system is available, was being used periodically by

[6] In the IRS's target architecture, the user identity and authenticator of each IRS employee will be stored on a smart card and used to access IRS facilities and information systems in accordance with HSPD-12.

users during their normal course of business. The remote logon software uses unencrypted communication and allows potential attackers to get access to usernames and passwords by listening on the network, which could lead to unauthorized access to the IFS. Further, the IFS did not have audit logging features enabled, as required by IRS security policy. Therefore, an attacker could gain unauthorized access to the IFS and steal or destroy financial records without being detected. The BSM organization informed us that it recently enabled audit logging features for the IFS application to mitigate this risk. Removing the BSM organization forest and authenticating IFS users through the IRS main production forest would eliminate this remote access vulnerability.

Further, the BSM organization forest impedes the IRS's goals for achieving consistent identity management user smart card access, in compliance with HSPD-12 requirements, because two logon accounts must be maintained for IFS users in the BSM organization forest and in their home forests.

The annual cost for the IBM Corporation contract is currently about $1.2 million. The original contract, made in Fiscal Year 2001, had been extended several times since Fiscal Year 2006; however, the extensions had not included upgrades to the existing equipment. The Microsoft Corporation ended support for Windows 2000 servers in July 2010; consequently, the IRS has spent $1.2 million from July 2010 to July 2011 to maintain obsolete equipment rather than spending those funds to resolve the vulnerability.

The BSM organization staff believes the best and least costly alternative for retiring the BSM organization forest is a Systems, Applications, and Products (SAP) in Data Processing Secure Network Communications[7] solution. However, this product has not yet been validated by the National Institute of Standards and Technology as Federal Information Processing Standards 140-2 compliant. The Federal Information Processing Standards Publication 140-2 specifies the security requirements that cryptographic[8] technologies must meet as standards for protection of sensitive or valuable data within Federal information systems. The National Institutes of Standards and Technology validates cryptographic technologies as meeting the standard, and precludes the use of unvalidated cryptographic technologies within Federal systems. The BSM organization informed us that it expects the SAP Secure Network Communications solution to achieve National Institute of Standards and Technology validation by December 2011, and to have it implemented by March 2012. The IRS approved funding to implement this solution in July 2011.

[7] SAP systems include basic security measures, which include the SAP authorization concept and user authentication based on passwords. With Secure Network Communications, SAP customers can extend SAP system security beyond these basic measures to include the additional protection offered by stronger authentication methods, by encryption, and by single logon.

[8] Cryptography refers to the transformation of ordinary text (plaintext) into coded form (ciphertext) by the use of encryption formulas and algothirims.

The effect to the IRS of allowing this separate BSM organization forest to remain includes:

- Increased security vulnerabilities because patches are no longer issued for Windows 2000 servers.
- The existing vulnerabilities in the legacy authentication method.
- The inability to leverage the centralized administration of configuration and access controls offered by the IRS main production domain.
- The dual logon environment impeding the IRS's goal of consistent identity management for complying with HSPD-12 requirements and IRS enterprise architecture security principles.

The four SOI organization forests are not needed to achieve stated goals of security and availability

The SOI organization collects, analyzes, and disseminates information on Federal taxation to various organizations engaged in economic and financial analysis and to the general public. The IRS Chief Technology Officer authorized the SOI organization to manage its own budget, infrastructure, and operations for the stated purpose of providing adequate security and availability of the statistical data it processes. When the SOI organization upgraded from its multiple Windows NT domain structure in January 2007, it installed a similar Active Directory configuration consisting of four separate forests, called SOIWORLD, SOINET, SOIPIN, and LIN. However, an implementation of four forests was not needed to achieve SOI organization goals of access control, data protection, and data availability. Rather, SOI organization goals for security and availability could be better achieved within the IRS main production forest.

SOI organization officials believe the four forests were needed to provide for the security principle of separation of duties. SOI organization officials indicated that if they were to collapse the four forests into one forest, several administrators would have access to all data within the entire SOI organization. They also stated that, because the administrators of each of the four forests only have administrative privileges over their respective forests, they can eliminate potential unauthorized access to sensitive data maintained in the other forests. In addition, the users of the different forests are also maintained in separated or segmented populations throughout the four-forest design. For example, the users of the LIN forest are mainly auditors, while the users of the SOIWORLD forest are comprised mostly of researchers. SOI organization officials believe this supports a clear and unambiguous need for separation of privileges within the SOI organization.

Separate forests are neither necessary nor sufficient to protect data from unauthorized access. Rather, sensitive resources should be protected with multiple levels of access controls with role separation implemented to ensure that an administrator with permission to manage one level of access control does not have permission to manage all levels. Rather than multiple forests,

domains within the common IRS Active Directory forest should be created to contain SOI organization resources, provide distinct administrative boundaries, and allow for customization of SOI organization-specific requirements while still adhering to IRS enterprise architecture security principles.

Further, SOI organization users have dual logon accounts, which create problems for the IRS moving towards an HSPD-12 smart card environment. SOI organization users possess an account in an SOI organization forest, to which they log on for performing their SOI organization duties, and an account in the IRS main production domain to which they log on for using common IRS services such as email and other service-wide resources. In order to advance the goal of consistent identity management and to maximize the value of the IRS Active Directory infrastructure, the SOI organization users' IRS main production logon credentials should be used as their sole Active Directory logon credentials for accessing SOI organization resources.

The SOI organization's implementation of four forests has resulted in inefficiencies relating to extra equipment, extra staff and man-hours to manage the additional equipment, the inability to take advantage of centralized management processes and technical solutions, and failure to meet the principles of the IRS enterprise architecture.

The nine ISRP organization forests cause management inefficiencies and unnecessary equipment

The ISRP application transcribes and formats data from paper tax returns and related documents for export to other IRS systems by key entry operators. It also captures check images for archiving. The IRS contracts with Lockheed Martin to manage the ISRP organization system code, though the IRS owns and manages the computer equipment and network that the ISRP organization system uses to perform its daily operations. In Fiscal Year 2003, when the ISRP organization converted from Windows NT to Active Directory, ISRP organization system administrators set up separate production forests at each of its six geographical sites where ISRP application processing occurs, generally to mirror how the former Windows NT domains were set up. They also implemented three forests for development, testing, and training. The ISRP organization staff stated that security would have to change if they went to a different configuration and, therefore, they stayed as close as possible to the current configuration.

While we agree that development and testing should generally be separated from a production environment, the ISRP organization did not utilize the administration efficiencies offered by consolidating its Active Directory infrastructure where possible. Minimizing the number of forests as much as possible would have allowed administration and security control from a centralized location and potentially realized significant savings by reducing duplicate support requirements. MITS organization staff informed us that the ISRP organization Windows Active Directory environment was designed by the ISRP contractors without consultation with the MITS organization staff who were charged with implementing the IRS's main production forest

in Fiscal Year 2005. In addition, the ISRP contractors have not ensured the ISRP Windows Active Directory environment has remained valid over time. Further, ISRP organization users have dual logon accounts, one for accessing the ISRP application and another for accessing the IRS main production forest, which creates problems for the IRS moving towards an HSPD-12 smart card environment and centralized and consistent identity and authentication management in adherence to IRS enterprise architecture security principles.

In addition, we identified inefficiencies related to network equipment at two ISRP production sites.

- Enterprise Networks organization staff at one of the six ISRP organization production sites described unneeded layers of ISRP routers and switches that provided an appearance of a separate ISRP network, although no real distinction between the ISRP network and the IRS network exists (i.e., they are one and the same). The Enterprise Networks organization staff took action to upgrade the ISRP routers and switches at that site because they often caused downtime and were noncompliant with IRS configuration requirements. At that time, the Enterprise Networks organization staff eliminated one router that was unnecessary. The Enterprise Networks organization staff believed this action was necessary because the ISRP vendor would not pay for the upgrade of equipment needed to meet IRS security requirements. This removal resulted in less downtime and the ability for the IRS to monitor that network components remain compliant with IRS standards.

  The Enterprise Networks organization staff advised us that the ISRP vendor also recently enabled Dynamic Host Configuration Protocol[9] services on two ISRP servers, which was unnecessary since the ISRP organization could use the IRS's Dynamic Host Configuration Protocol servers. The Enterprise Networks organization staff stated that, in general, the ISRP vendor claims it needs control over the network and its components in order to guarantee its performance under its contract. The Enterprise Networks organization staff believed efficiencies could be realized if local IRS staff were allowed to support and manage the network components at the other ISRP organization sites.

- Enterprise Networks organization staff at another ISRP organization production site advised us that ISRP organization routers and switches there have also introduced unnecessary complications to the network infrastructure, as well as introducing additional points of failure. The Enterprise Networks organization staff's professional opinion was that the ISRP organization routers are unnecessary. The Enterprise Networks organization staff indicated that the switches are necessary but could easily be replaced

[9] A protocol for assigning dynamic Internet Protocol addresses to devices on a network. Dynamic addressing simplifies network administration because the software keeps track of Internet Protocol addresses rather than requiring an administrator to manage the task.

by IRS switches. This replacement would serve to flatten the network, improve management, and provide local technicians the ability to troubleshoot.

The Enterprise Networks organization staff stated that it currently has no view into the ISRP organization network, including its routers and switches, or access to these devices. As a result, they are unable to assist the user community when trouble occurs. However, the Enterprise Networks organization staff has the responsibility to replace faulty routers and/or switches when ISRP organization contractors determine replacements are needed. This situation requires Enterprise Networks organization staff to rely on ISRP organization contractors to have completed thorough and competent troubleshooting before determining a replacement is needed. Further, the Enterprise Networks organization staff informed us that ISRP organization routers and switches have also caused additional, and unnecessary, complications to the workstation configurations. The Enterprise Networks organization staff stated that the ISRP organization network design is faulty in that it requires all workstations to be manually configured, resulting in a poorly designed version of load balancing.[10] The Enterprise Networks organization staff believed the ISRP organization should be using Dynamic Host Configuration Protocol to configure network parameters on its workstations, alleviating the need to do this work manually that is resource intensive.

The ISRP organization Program Office staff advised us that the ISRP organization contract expires in Fiscal Year 2012. The IRS should consider implementing changes to the ISRP organization contract that would allow the IRS to improve on the current administration and network inefficiencies caused by operating an application across multiple forests.

We believe the unnecessary separate BSM, SOI, and ISRP organizations' forests exist because the IRS did not finalize its policy for forest design nor enforce its Active Directory network topology in compliance with its enterprise architecture security principles.

Inefficiencies related to extra forests include the installation of extra equipment, additional staff required to manage the excess infrastructure, and the inability to centrally assign enterprise-wide policies and apply critical updates, which impedes the IRS from achieving its goal of consistent identity management and HSPD-12 requirements. Consolidating unnecessary forests would allow administration and security control from a centralized location and potentially realize significant savings by reducing duplicate support requirements.

[10] Load balancing is a computer networking methodology to distribute workload across multiple computers or other resources to achieve optimal resource utilization, maximize throughput, minimize response time, and avoid overload.

Recommendations

The Chief Technology Officer should ensure that:

Recommendation 1: The MITS organization establishes an enterprise-wide Active Directory governing body that finalizes and enforces IRS Active Directory forest design criteria, develops standards, oversees trusts, and ensures unauthorized forests or domains are not implemented in the IRS.

> ***Management's Response:*** The IRS agreed with this recommendation. The MITS organization will establish an Active Directory governing body to finalize and enforce IRS Active Directory forest design criteria, standards, oversee trusts, and ensure unauthorized forests or domains are not implemented in the IRS.

Recommendation 2: The planned shutdown of the BSM forest is completed once the SAP Secure Network Communications solution is in place. The SOI and ISRP organizations should work with the MITS organization to perform a feasibility study to determine if the collapse of the SOI and ISRP forests is practical and in the best interest of the IRS. If deemed in the best interest of the IRS, the MITS organization should prepare plans with funding requirements and potential completion dates to accomplish the collapse of one or both of these organizations' forests.

> ***Management's Response:*** The IRS agreed with this recommendation. The MITS organization will complete the shutdown of the BSM forest after the deployment of the SAP Secure Network Communications solution is in place. Additionally, the MITS organization will work with the ISRP and SOI organizations to study the costs, staffing, and technical issues involved in the collapse of these forests into the IRS main Active Directory forest. If it is deemed practical and in the best interest of the IRS and the business unit to collapse the forests, the MITS organization will work with the ISRP and SOI organizations to determine the project(s) and timeline to accomplish the work within overall project priorities and available funding. As it relates to the SOI forest, the IRS will address specific guidelines for Federal Statistical Agencies to protect the confidentiality of the data as set forth in the Confidential Information Protection and Statistical Efficiency Act, which was signed into law under Title V of the E-Government Act of 2002.
>
> ***Office of Audit Comment:*** The IRS did not agree with the outcome measure (see Appendix IV) relating to the expenditure of $1,200,000 in contract fees to maintain obsolete computer equipment in the BSM forest. In its response, the IRS stated that the computer equipment was required to support critical financial and accounting management functions and that these functions would have stopped had the monies not been spent. The IRS agreed that the computer equipment needs to be updated, and a plan has been formulated to do so in Fiscal Year 2012. However, we contend that the IRS

should have been aware of the July 2010 date when Microsoft ended its support for these types of computers, and that the IRS did not act in due diligence to formulate an update plan prior to that date in order to resolve the vulnerability caused by these obsolete computers. Therefore, the IRS's expenditure of funds to maintain the obsolete computer equipment that put critical functions at risk rather than spending those funds to resolve the vulnerability was an inefficient use of resources.

Not All Windows Servers and Workstations Connected to the Network Reside in Authorized Domains

IRS policy requires that all computers connected to the IRS network reside in an approved domain, except for public web servers. Domains are groups of computers on a network within a forest that are administered as a unit with common rules and procedures. Managing Windows servers in Active Directory domains offers a centralized and efficient method for applying and managing security controls on all computers residing in the domain.

In December 2008, the MITS Enterprise Operations organization created a standard in order to prevent servers from being connected to the network without the proper authorization and required compliance documentation, as well as prevent unauthorized domains from being created. The Associate Chief Information Officer, Enterprise Operations organization, is responsible for establishing, maintaining, and enforcing this standard for all Windows servers connected to the IRS network. This standard authorizes the identification and reporting to the Associate Chief Information Officer (or designee), Enterprise Operations organization, and applicable business owners of any noncompliant server if one or more of the following conditions apply:

1. Is identified as operating on the IRS network without being documented as a part of an IRS general support system, or having its own security certification, or otherwise being authorized/certified to operate by the MITS Cybersecurity organization.
2. Is not in compliance with the security settings defined in the Internal Revenue Manual and Enterprise Operations organization security configuration standard as appropriate for the server's operating system.
3. Does not have the required server information entered in the Enterprise Operations Server Database, including an organization designated as the server owner, the domain to which the server belongs (or will belong), the general support system to which the server belongs, and a point of contact for the server.
4. Is a member of an unauthorized domain. Servers in unauthorized domains, as well as the domains themselves, are subject to removal from the network.

Based on network scans performed by the IRS in November 2010, the Business DNA[11] asset discovery tool identified 772 Windows servers and 238 workstations, in a total of 71 uniquely named domains or groups, residing on the IRS network but outside of the administrative boundaries established by the Enterprise Operations, Chief Counsel, Criminal Investigation, Computer Security Incident Response Center, SOI, BSM, and ISRP organizations. The Business DNA scanning tool identifies computers and other devices that are active on the network at the point in time the scan occurs. Figure 2 provides a list of unidentified domains or groups with servers and/or workstations on the IRS network. This list may not be all-inclusive of servers and workstations residing outside of recognized domains.

Figure 2: List of Unidentified Domains or Groups With Servers and/or Workstations on the Network

Unidentified Domains or Groups	Number of Windows		Unidentified Domains or Groups	Number of Windows	
	Servers	Workstations		Servers	Workstations
ADCW2K	2	0	METRO1	4	0
ADPOC	1	0	METRO2	5	0
ALARMPOINT	4	0	METRO3	1	0
AMSHLD	0	1	MSHOME	0	1
ANDOVERSEC	2	0	MTCNC	0	1
ASPECTCC	83	0	MTCSBX	2	0
BLN004-WG	4	0	NC	0	1
CIO	1	0	NEW	0	1
CLEARPATH	2	0	PEDRO	0	1
DALLAS-LAB	1	0	PSC003	4	0
DEVNET	1	1	PUE75A	2	0
DTS	37	0	RESEARCH	7	0
EA	3	0	ROADMAP	7	0
ENCIL	1	0	ROADMAP2	3	1
EPPM	3	0	SBX2	1	0
GEOIRS	233	3	SBX2.PRIME.IRS.GOV	1	0
IE-LAB	1	0	SECURITY	1	7
INTERVOICE	1	0	T	2	0

[11] Business DNA is an asset discovery tool that provides detailed hardware and software configuration information for all devices connected to the network. The Department of the Treasury recently selected Business DNA as the enterprise tool for all bureaus to use in information technology asset discovery, inventory, and reporting.

Unidentified Domains or Groups	Number of Windows		Unidentified Domains or Groups	Number of Windows	
	Servers	Workstations		Servers	Workstations
INTRUSHIELD	1	0	TACACS-EXT	2	0
IPT	16	1	TACACS-INT	3	0
IPTELEPHONY	1	0	TEMP	1	0
IRS	16	3	TEST	0	1
IRS_WORKGROUP	1	0	TMPWORK	3	6
IRSERAP	2	0	VDE	1	0
IRSIPTELEPHONY	5	4	VELOCITY	0	1
IRS-IPTELEPHONY	9	0	VGNOC	2	0
IRS-IPTELEPHONYI	5	0	VOIP	7	2
IRSKCSC	2	0	VVV	0	1
IRSODN001BERBEEI	1	0	W	0	1
IRSOGDENCCM	1	0	WG	0	3
IRSOGDENIPT	1	0	WORK	0	1
IRS-TELEPHONY	2	0	WORKGROUP	250	193
LAB_TEST	1	0	WORKGROUPX	2	0
LMSB	0	1	WRKGR	0	1
MDI	7	0	WW	0	1
MDI-3166	10	0		**Servers**	**Workstations**
TOTALS				772	238

Source: Results of Business DNA network scan the IRS performed in November 2010.

We selected a judgmental sample of 12 servers from this list and requested the Enterprise Operations organization determine whether or not the domains or groups they were residing in were authorized. Of these 12 servers, the Enterprise Operations organization did not recognize the domain or group name for 7 of them nor could it determine the owner or purpose of these servers. The server information had not been entered in the Enterprise Operations organization Server Database, and none had the Tivoli®[12] software installed. At the time Enterprise Operations organization performed its research on these servers in April 2011, all but one of the seven servers were still active on the IRS network.

[12] Tivoli is a registered trademark owned by the IBM Corporation. The implementation of Tivoli is part of the IRS Enterprise Systems Management project encompassing helpdesk operations, network and systems management, software distribution, asset management, and performance measures analysis and reporting.

Enterprise Operations organization officials informed us that valid reasons may exist for some of these domains and groups, but it would take massive man hours to research them to make this determination. Valid reasons for keeping computers in separate IRS forests and domains could include, for example, the need to isolate computers that protect the IRS from internet attacks, or to contain computers that are too old to operate in an Active Directory environment. Enterprise Operations organization officials also stated that while they created standards to prevent unauthorized domains from being created and servers from being connected to the network without the proper authorization, no central controlling authority over domain creation or approval exists at the IRS to ensure compliance with Enterprise Operations organization standards.

A lack of control over domain creation defeats the efficiencies the MITS organization intended to achieve when implementing one shared administrative boundary for the majority of IRS resources. In addition, if not part of an approved domain, these servers and workstations may be at increased risk of noncompliance with IRS security policy, putting the IRS at risk of security breaches.

Recommendations

The Chief Technology Officer should ensure that:

Recommendation 3: Standards and processes are developed and implemented enterprise-wide to prevent servers and workstations from being connected to the network without the proper authorization and required compliance documentation.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS will ensure that standards and processes are developed and implemented enterprise-wide to prevent servers and workstations from being connected to the network without proper authorization and required compliance documentation.

Recommendation 4: Scanning tools, such as the Business DNA, are utilized to locate unauthorized servers, workstations, and domains on the IRS network, and adequate procedures are developed and implemented to ensure they are removed.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS will use automated scanning tools for asset identification and has been in the process of implementing this capability, even prior to this audit. The IRS will also ensure that IRS policy addresses the issue of proper handling and potential removal of any unauthorized assets found, regardless of how they are discovered.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether the IRS has structured its Windows environment to provide efficient and secure management of Windows servers. To accomplish the objective, we:

I. Evaluated the IRS Active Directory environment to determine whether its structure provided efficient and secure management of Windows servers.

A. Determined whether the IRS effectively controlled the creation of Active Directory forests[1] in its Windows environment.

1. Obtained IRS Windows servers inventory and forest design data from the IRS personnel responsible for managing them.

2. Documented the IRS Windows environment, including the number of forests, domains, and Windows servers.

B. Interviewed IRS personnel responsible for currently known forests and made a conclusion on whether each met IRS criteria for establishing a forest.

1. Determined whether each forest was considered appropriate by the MITS Enterprise Services, System Architecture and Engineering organization.

2. Determined whether each forest met IRS criteria for establishing a separate forest.

C. Obtained Business DNA scan data and analyzed the additional forests, domains, and servers it identified.

1. Interviewed IRS staff to determine whether the additional forests, domains, and servers identified by the Business DNA scan data were authorized.

2. Selected a sample of 12 servers from the population of 772 servers that the Business DNA scan identified that were not included in the inventory listings of servers provided by the IRS. We judgmentally selected the 12 servers due to time constraints and the time-intensive research required to determine whether or not the forests, domains, or groups they were residing in were authorized.

3. Determined the causes that allowed the creation of any unauthorized forests, domains, and servers.

[1] A forest is the outermost design element or boundary in an Active Directory·

4. Determined the effects any unauthorized forests, domains, and servers had on the IRS Windows environment.

D. Determined whether the IRS had adequate policy for controlling the creation of Windows forests.

1. Obtained current IRS policy for the creation of forests and determined whether it was adequate to control the creation of unnecessary forests.
2. Interviewed IRS staff to determine why the IRS policy for the creation of forests was not complete or adequate.

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 determined the following internal controls were relevant to our audit objective: IRS policy and procedures for Windows server security and creation of Active Directory infrastructure. We evaluated these controls by interviewing IRS personnel, reviewing Active Directory design documents, obtaining Windows server inventories, and analyzing network scan data.

Appendix II

Major Contributors to This Report

Alan Duncan, Assistant Inspector General for Audit (Security & Information Technology Services)
Kent Sagara, Director
Jody Kitazono, Audit Manager
George Franklin, Senior Auditor
Midori Ohno, Senior Auditor
Ashley Weaver, Auditor
Elton Jewell, 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
Deputy Commissioner for Services and Enforcement SE
Director, Office of Research, Analysis and Statistics RAS
Chief Counsel CC
Chief, Criminal Investigation SE:CI
National Taxpayer Advocate
Associate Chief Information Officer, Cybersecurity OS:CTO:C
Associate Chief Information Officer, Enterprise Operations OS:CTO:EO
Director, Statistics of Income RAS:S
Director, Office of Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Office of Internal Control OSCFO:CPIC:IC
Audit Liaison: Director, Risk Management Division OS:CTO:SP:RM

Appendix IV

Outcome Measure

This appendix presents detailed information on the measurable impact that our recommended corrective actions will have on tax administration. This benefit will be incorporated into our Semiannual Report to Congress.

Type and Value of Outcome Measure:

- Inefficient Use of Resources – Potential; $1,200,000 in contract fees (see page 4).

Methodology Used to Measure the Reported Benefit:

From July 2010 to July 2011, the IRS spent $1,200,000 on a contract with the IBM Corporation to provide computer equipment that serves to authenticate users to the IFS[1] application. The computers are primarily Windows 2000 servers. The Microsoft Corporation ended support for Windows 2000 servers in July 2010 and no longer issues patches to protect the servers from known vulnerabilities. Consequently, the IRS has spent $1,200,000 to maintain obsolete servers that are a high security risk.

[1] The IFS manages the IRS's $11.4 billion operating budget for administering tax payments, collection, and enforcing tax laws.

Appendix V

Management's Response to the Draft Report

CHIEF TECHNOLOGY OFFICER

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

SEP 13 2011

RECEIVED
SEP 13 2011

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Terence V. Milholland
Chief Technology Officer

SUBJECT: Draft Audit Report –Continued Centralization of the Windows Environment Would Improve Administration and Security Efficiencies (Audit # 201120010) (e-trak # 2011-24397)

Thank you for the opportunity to review and respond to the subject audit report. We appreciate your comments.

We agree with the four recommendations in the report. However, we do not agree with the outcome measure. We disagree that the expenditure of $1,200,000 for IFS computer equipment represents an inefficient use of resources. The computer equipment TIGTA identified is required to support critical financial management and accounting functions. If the IRS had not spent the monies, those functions would have stopped thereby placing financial processing in jeopardy. The IRS acknowledges that IFS computer equipment needs to be updated and a plan has been formulated to accomplish this in Fiscal Year 2012.

We value your continued support and the guidance your team provides. If you have any questions, please contact me at (202) 622-6800 or Andrea Greene-Horace, Senior Manager of Program Oversight, at (202) 283-3427.

Attachment

Draft Audit Report – TIGTA Draft Report – Continued Centralization of the Windows Environment Would Improve Administration and Security Efficiencies (Audit # 201120010) (e-trak # 2011-24397)

RECOMMENDATION #1: The Chief Technology Officer should ensure that the MITS organization establishes an enterprise-wide Active Directory® governing body that finalizes and enforces IRS Active Directory® forest design criteria, develops standards, oversees trusts, and ensures unauthorized forests or domains are not implemented in the IRS.

CORRECTIVE ACTION #1: We agree with the recommendation. MITS will establish an Active Directory® governing body to finalize and enforce IRS Active Directory® forest design criteria, standards, oversee trusts, and ensure unauthorized forests or domains are not implemented in the IRS.

IMPLEMENTATION DATE: July 1, 2012

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Operations

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

RECOMMENDATION #2: The Chief Technology Officer should ensure that the planned shutdown of the BSM forest is completed once the SAP Secure Network Communications solution is in place. The SOI and ISRP organizations should work with the MITS organization to perform a feasibility study to determine if the collapse of the SOI and ISRP forests is practical and in the best interest of the IRS. If deemed in the best interest of the IRS, the MITS organization should prepare plans with funding requirements and potential completion dates to accomplish the collapse of one or both of these organization's forests.

CORRECTIVE ACTION #2: We agree with the recommendation. MITS will complete the shutdown of the BSM Forest after the deployment of the SAP Secure Network Communications solution is in place. Additionally, MITS will work with the ISRP and SOI organizations to study the costs, staffing and technical issues involved in the collapse of these forests into the IRS main Active Directory forest. Therefore, if deemed practical and in the best interest of the IRS and the business units to collapse the forests, MITS will work with the organizations to determine the project(s) and timeline to accomplish the work within overall project priorities and available funding. As it relates to the SOI forest, we will address specific guidelines for Federal Statistical Agencies to protect the confidentiality of the data as set forth in the Confidential Information Protection and Statistical Efficiency Act (CIPSEA) which was signed into law under Title V of the E-Government Act of 2002.

Draft Audit Report – TIGTA Draft Report – Continued Centralization of the Windows Environment Would Improve Administration and Security Efficiencies (Audit # 201120010) (e-trak # 2011-24397)

IMPLEMENTATION DATE: November 1, 2012

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Operations

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

RECOMMENDATION #3: The Chief Technology Officer should ensure that standards and processes are developed and implemented enterprise-wide to prevent servers and workstations from being connected to the network without the proper authorization and required compliance documentation.

CORRECTIVE ACTION #3: We agree with the recommendation. The IRS will ensure that standards and processes are developed and implemented enterprise-wide to prevent servers and workstations from being connected to the network without proper authorization and required compliance documentation.

IMPLEMENTATION DATE: May 1, 2013

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

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

RECOMMENDATION #4: The Chief Technology Officer should ensure that scanning tools, such as the BDNA, are utilized to locate unauthorized servers, workstations, and domains on the IRS network, and adequate procedures are developed and implemented to ensure they are removed.

CORRECTIVE ACTION #4: We agree with the recommendation to use automated scanning tools for asset identification and have been in the process of implementing this capability, even prior to this audit. IRM 2.14.1 defines the process for inventory reconciliation of all IT assets. The IRS will ensure that the IRM addresses the issue of the proper handling and potential removal of any unauthorized assets found, regardless of how discovered.

Draft Audit Report – TIGTA Draft Report – Continued Centralization of the Windows Environment Would Improve Administration and Security Efficiencies (Audit # 201120010) (e-trak # 2011-24397)

IMPLEMENTATION DATE: October 2, 2012

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

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