TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

The Enterprise-Wide Implementation of Active Directory® Needs Increased Oversight

May 2006

Reference Number: 2006-20-080

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

Phone Number | 202-927-7037
Email Address | Bonnie.Heald@tigta.treas.gov
Web Site | http://www.tigta.gov

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

May 9, 2006

MEMORANDUM FOR CHIEF INFORMATION OFFICER

FROM: Michael R. Philips
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The Enterprise-Wide Implementation of Active Directory® Needs Increased Oversight (Audit # 200520010)

This report presents the results of our review to determine whether the Internal Revenue Service (IRS) had effectively and securely implemented the Active Directory®-based network and the Windows 2003® Server Operating System.

Synopsis

The IRS is in the process of implementing an Active Directory®-based network and upgrading its computers to the Windows 2003® Server Operating System. Active Directory® is the Microsoft Corporation's (Microsoft) latest technology for administering and securing computer networks and is a central component of the Windows 2003® Server Operating System. Active Directory® manages the identities and relationships of computing resources that comprise a network, simplifies system administration, and provides easier methods to strengthen and consistently secure computer systems. Because the IRS' previous network operating system was divided into obsolete and inefficient boundaries, expensive to manage, and difficult to consistently secure, the migration to Active Directory® should result in an upgraded network that can better meet the IRS' future needs.

The IRS has made significant progress in its Active Directory® implementation; however, increased oversight is needed to ensure the IRS achieves all expected benefits, including more efficient network management and increased security.

The IRS has made significant progress in implementing Active Directory®. Planning began in Fiscal Year 2000, and the IRS expects to complete the migration by December 31, 2006. However, significant risks remain that must be addressed for

the IRS to achieve the benefits of Active Directory®. For example, design standards must be enforced. Ideally, all IRS functions could be included within one boundary (called a forest[1] in Active Directory®). However, managers and system administrators, who play a large role in managing current domains[2] and applications, may be reluctant to participate in the IRS Active Directory® forest since they will likely lose autonomous control over the network components. Five Active Directory® forests have already been established, and two IRS organizations have stated a need for additional separate forests. Adding unnecessary separate forests will increase the cost of implementing and maintaining Active Directory® and will make maintaining consistent security controls more difficult. Funding must also be provided to replace outdated computers that cannot support Active Directory®. In addition to the costs of the computers, the IRS is paying Microsoft custom support fees to support its outdated operating systems until the computers are replaced.

The Active Directory® Team did not have sufficient authority to finalize Active Directory® guidance documents, enforce adherence to design and security standards and industry best practices, and ensure the timely and successful migration of Active Directory® IRS-wide. During our review, the IRS formed a new project team with executive leadership that can provide the level of oversight needed to ensure the successful implementation of Active Directory®. Because the new team and leadership are already aware of these implementation issues, we made no recommendations to address these issues.

We also found some of the computers that had been migrated into the new Active Directory®-based network did not meet the IRS' approved security standards. We reviewed a sample of 53 servers[3] from the 399 that had been migrated to the Active Directory®-based network at the time we initiated our review in July 2005. Over 22 percent did not adequately comply with the IRS' approved security settings, resulting in vulnerabilities that could be exploited by hackers and disgruntled employees. In some instances, Active Directory® security settings were changed to what the IRS considered stronger settings or to enable the servers to perform a particular role on the network. In both instances, changes were made without obtaining concurrence from the Chief, Mission Assurance and Security Services, and approval from the system owner, as required.

In addition, sufficient oversight was not provided over system administrator accounts. These accounts need to be carefully controlled because they are the most powerful accounts that exist on the network and can perform critical tasks that have major effects on the security, operation, and performance of the network. We found:

[1] The forest is the outermost boundary of Active Directory®.
[2] Domains are groups of computers on a network that are administered as a unit with common rules and procedures.
[3] Servers are computers that carry out specific functions. For example, file servers store files, print servers manage printers, and network servers manage network traffic.

- Unnecessary system administrator accounts had been created on 49 percent of the servers we tested. Accounts for these employees should have been created in a central system administrator group to improve the management of the accounts and to improve security.
- Built-in system administrator accounts were not being adequately safeguarded. System administrators must disguise these powerful accounts to prevent intruders from identifying them. While the IRS' security standards require these accounts to be renamed to help hide them, the new names did not adequately disguise these accounts on 57 percent of the servers we tested. In addition, the nature of these accounts was still readily apparent on all 53 sampled servers because, directly next to the account names, there were descriptions labeling them as built-in system administrator accounts.

Recommendations

We recommended the Chief Information Officer develop a formal process for approving deviations from the IRS' approved security settings for Active Directory®. When deviations are preferred or needed, concurrence from the Chief, Mission Assurance and Security Services, and approval of the system owner should be requested. We also recommended the Chief Information Officer improve oversight of system administrator accounts during the implementation of Active Directory®. Computers should be periodically reviewed for compliance with requirements. Procedures should be enforced and system administrators held accountable for adhering to these procedures.

Response

IRS management agreed with our recommendations. Requests for deviations will include the recommendation from the Chief, Mission Assurance and Security Services, and approval from the system owner. The IRS will increase oversight of system administrator accounts and enforce procedures for protecting them. Computers will be periodically monitored and system administrators will be held accountable for complying with procedures. Management's complete response to the draft report is included as Appendix IV.

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

Table of Contents

Background

In today's information technology environment, networked computing is essential for organizations to remain effective and efficient. As a result, modern operating systems require a directory service for managing the identities and relationships of the resources that reside on networks. A directory service:

- Stores information about a network's applications, files, and printers and the people who have access to the network.
- Provides a consistent way to name, describe, access, manage, and secure information about these resources.
- Acts as the main switchboard of the network operating system.

Because a directory service supplies these fundamental network operating system functions, it must be tightly coupled with the operating system controls to ensure the integrity and privacy of the network.

The Internal Revenue Service (IRS) operates a large computer network that includes about 3,000 servers[1] and 110,000 workstations using Windows® operating systems provided by the Microsoft Corporation (Microsoft). Until recently, the IRS network was divided into over 100 domains[2] that were based on obsolete and inefficient organizational boundaries, resulting in high operating costs and inconsistent security controls. The IRS' domain structure lacked the flexibility, scalability,[3] and power needed to support changes in organizational needs.

In 2000, the IRS began addressing these concerns by planning the deployment of Active Directory®, Microsoft's latest technology for administering and securing computer networks. In addition to strengthening security, Active Directory® can simplify system administration by providing a single, consistent point to manage users, applications, and devices. It provides users with a single sign-on to network resources and provides system administrators with powerful tools to ensure consistent security controls among desktop users, remote dial-up users, and external e-commerce customers.

[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.
[2] Domains are groups of computers on a network that are administered as a unit with common rules and procedures.
[3] Scalability is a term that refers to how well a system can adapt to increased demands. A scalable network can start with a few computers and network devices and can easily expand to thousands. Scalability means an organization will not outgrow its system.

Active Directory® is a pervasive technology that affects virtually the entire IRS network. Its implementation is a major undertaking due to the size of the IRS network and the diversity of IRS functions it supports. The IRS is currently in the process of upgrading its computers from the Windows NT® operating system to the Windows 2003® Server Operating System and moving them into the Active Directory®-based network. When we initiated this review in July 2005, the migration was still in process and the IRS had moved 399 servers to the new network. The IRS expects to move all 110,000 workstations in early 2006 and all 3,000 servers by December 31, 2006.

This review was performed at the Active Directory® Team offices within the Modernization and Information Technology Services organization's[4] End User Equipment and Services organization[5] in Boston, Massachusetts, and Atlanta, Georgia, during the period July through September 2005. The audit was conducted in accordance with *Government Auditing Standards*. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

[4] The Modernization and Information Technology Services organization leads the delivery of IRS information technology solutions to meet enterprise-wide customer needs by providing information technology systems, products, services, and support.
[5] The End User Equipment and Services organization is a part of the IRS Modernization and Information Technology Services organization and provides end user computer products, services, and support to IRS functions.

Results of Review

The IRS has made significant progress in implementing Active Directory® and is on schedule for migrating user accounts, workstations, and servers into the new network. However, significant risks remain that must be addressed for the IRS to achieve the benefits of Active Directory®, specifically to simplify system administration and strengthen overall security.

Actions Are Needed to Allow Active Directory® to Simplify System Administration

For the past several years, a team of about 20 members from the End User Equipment and Services organization has driven the design and deployment of the Active Directory®-based network for most of the IRS. The Active Directory Team developed design documents and implementation plans for the new Active Directory®-based network in accordance with Microsoft recommendations and industry best practices. While the Team has made significant progress, its members advised, and we confirmed, it did not have the cross-functional authority to ensure all IRS entities were working together, including the Modernization and Information Technology Services organization, the Office of Mission Assurance and Security Services,[6] and the IRS business units. The Team did not have the authority to finalize guidance documents, enforce adherence to design and security standards, or ensure timely and successful implementation of Active Directory® IRS-wide.

After we discussed these concerns with lead members of the Active Directory® Team, the IRS formed a new project team with the authority to address Active Directory® design and security issues from an enterprise perspective. The new team is led by the Enterprise Services organization[7] and reports to the Infrastructure Executive Steering Committee.[8] We concur with this approach and believe the Steering Committee can provide the executive-level oversight needed to implement Active Directory®. To achieve the full system administration benefits of Active Directory®, the Steering Committee will need to enforce design standards and provide adequate funding and oversight to keep implementation on schedule. Because the Steering Committee is already aware of these implementation issues, we are making no recommendations to address these issues.

[6] The Office of Mission Assurance and Security Services is a service and support organization that assists the IRS operating divisions in maintaining secure facilities, technology, and data.
[7] The Enterprise Services organization is a part of the Modernization and Information Technology Services organization and manages common information technology functions and services performed across the IRS.
[8] The Infrastructure Executive Steering Committee oversees the technological infrastructure for building modernized systems.

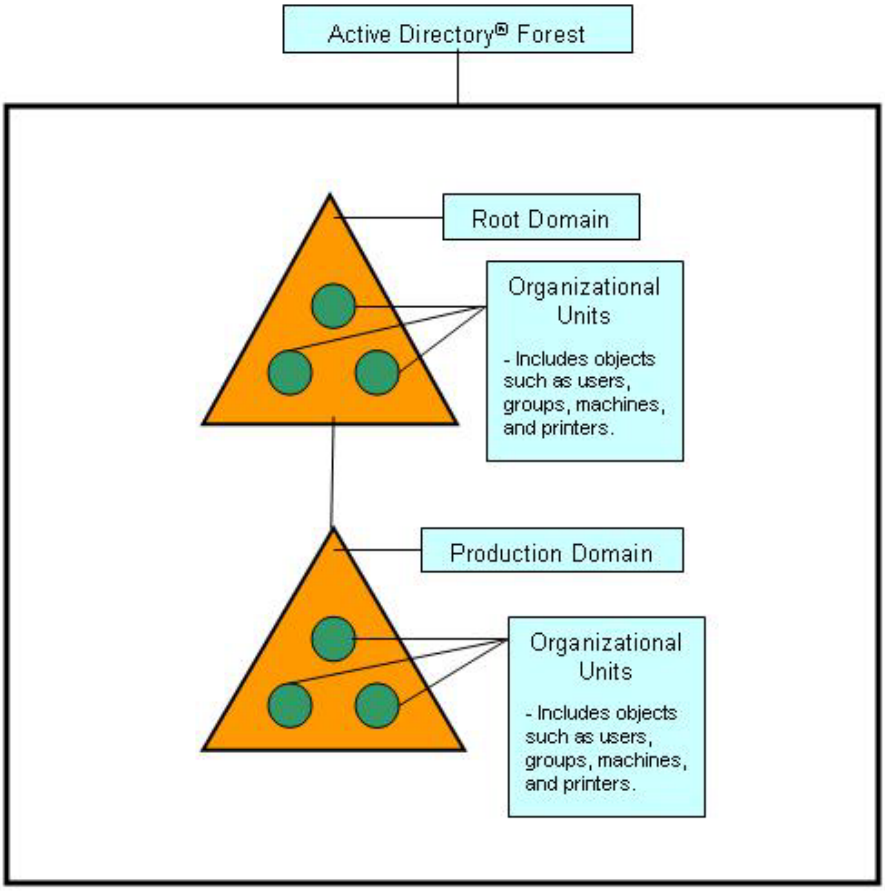
Active Directory® design standards must be enforced

The large and dispersed network used by the IRS often requires time-consuming and redundant system administration. Active Directory® allows the IRS to significantly lower system administration costs by providing a single place to manage users, groups, and network resources, as well as to distribute software and manage desktop configurations. It automatically distributes software to users based on the users' roles, thus reducing or eliminating multiple contacts the system administrators need to make to employees' workstations to install and configure software.

Active Directory® uses a hierarchical approach to allow organizations to more easily administer the entire network and to customize administration based on the needs of users. Active Directory® refers to its outermost logical boundary as a forest. A forest is a collection of subsets that share the same Active Directory® configuration and design elements. These subsets are called domains. Domains are used to manage the various populations of users, computers, and other network resources.

A best practice is to create a large "production domain" to hold almost all of an organization's users and computers. A smaller "root domain" is created to contain a minimal number of powerful administrative accounts and computers. Within domains, smaller subsets called "organizational units" are used to create administrative groupings of users, computers, and printers that can be uniformly managed. Figure 1 depicts the various levels in the Active Directory® hierarchy.

Figure 1: Illustration of a Common Active Directory® Structure



Source: The Treasury Inspector General for Tax Administration's depiction based on Microsoft documentation.

Ideally, the IRS could maintain one forest, then use domains and organizational units to group objects that have common system settings based on specific needs of the various IRS functions. Separate forests add overhead and are less efficient because they require the creation and maintenance of additional design elements and security components, whereas adding an entity to an existing forest takes advantage of existing design elements and security components.

The Active Directory® Team established the main IRS production forest and provided criteria in accordance with industry best practices for justifying additional forests. IRS entities requesting a separate forest must have stringent security requirements, such as the maintenance of law enforcement data, that require elevated security clearance for system administrators.

To date, the IRS has been successful at limiting the number of forests. Most network resources are included in a single forest with a root domain and one large production domain.

Additional forests have been created for two IRS functions (the Offices of Chief Counsel and Criminal Investigation) and one system (the Integrated Submission and Remittance Processing System[9]) that need greater security and can justify the need for separate forests. A forest was also created for the Integrated Financial System[10] because it was implemented before the IRS was ready to deploy Active Directory® on an enterprise-wide basis. However, this system does not meet the IRS' criteria for establishing a separate forest; therefore, consideration should be given to bringing it into the IRS' main production forest to achieve maximum efficiencies and security of IRS operations.

As the implementation of Active Directory® continues, we expect other entities will request separate forests. Managers and system administrators who play a large role in managing current domains and applications may be reluctant to participate in the IRS Active Directory® forest since they will likely lose autonomous control over the network components. For example, two IRS organizations have stated a need for separate Active Directory® forests in addition to the five forests already established. Adding unnecessary separate forests will increase the cost of implementing and maintaining Active Directory® and will make maintaining consistent security controls more difficult.

Funding must be provided to ensure Active Directory® implementation remains on schedule

The IRS must also allocate sufficient funds to achieve the benefits of Active Directory®. Most of the advanced security features offered by Active Directory® cannot be implemented until outdated computer workstations and servers that cannot support Active Directory® are updated or replaced. Salary costs for upgrading or replacing servers and workstations were approximately $5.2 million in Fiscal Year 2005, and an additional $2.4 million is estimated to be spent in Fiscal Year 2006. In addition, the IRS must continue to pay Microsoft to support its outdated operating system. After Microsoft support for the IRS' current network operating system ended in December 2004, the IRS paid for custom support so it could continue to receive security patches costing about $318,000 through December 2005. Because computers with the old operating system are not expected to be upgraded and migrated into Active Directory® until December 31, 2006, the IRS plans to continue custom support agreements costing $100,000 for each 6-month period those computers are operating. Delays in updating or replacing the outdated workstations and servers will not only postpone the benefits of Active Directory® but also force the IRS to pay additional support costs for its outdated operating system.

We also noted resources and funding for a separate forest to be used as a testing environment had not been sufficient. IRS security standards require testing to be done separately from the

[9] The Integrated Submission and Remittance Processing System processes paper returns and payments submitted by taxpayers.
[10] The Integrated Financial System gives the IRS timely and easier access to accurate and consistent financial data, resulting in improved decision making and management.

production environment. Because the IRS did not fund a separate testing forest, testing was performed in the production forest and in unauthorized test domains that were not compliant with IRS security policies, expensive to maintain, and likely do not represent the production forest. As a result, testing could disrupt the production environment and produce unreliable results.

Actions Are Needed to Enable Active Directory® to Strengthen Network Security

Strong and consistent security controls are essential to protect the confidentiality, integrity, and availability of sensitive taxpayer data maintained on the IRS network. Active Directory® centralizes system administration and enforces role-based access controls that can be applied to both desktop and remote users. To take advantage of Active Directory® capabilities to strengthen the security of the IRS network, the IRS should ensure security settings on servers are enhanced, system administrator access rights are controlled, system administrator accounts are securely managed, and built-in system administrator accounts are safeguarded.

Server security settings did not always comply with IRS standards

The IRS has standard security settings for many types of computers. Active Directory® provides new techniques for consistently applying these settings. Computers that need to be similarly secured are placed in a group, called an organizational unit. Customized security settings needed for computers in a particular organizational unit are placed into one or more subsets, called group policy objects. Security settings are consistently applied to all the computers by linking the organizational unit to the corresponding group policy objects. Any computer subsequently added to the organizational unit should automatically receive the appropriate security settings. Deviations from the standard settings must be concurred with by the Chief, Mission Assurance and Security Services, and approved by the system owner.

Because IRS servers have various roles, the Active Directory® Team created an organizational unit for each role. The IRS also created a group policy object containing universal security settings, which are applied to all of its server organizational units, and several specialized group policy objects containing additional settings, which are applied to only specific server organizational units.

In our sample of 53 servers moved to the Active Directory®-based network, 12 (22.6 percent) did not adequately comply with the IRS' approved settings. Six servers did not adequately comply because the organizational unit in which they were located was not linked to a group policy object. The Active Directory® Team deleted this organizational unit from the Active Directory® before our audit had been completed. Five servers were in organizational units linked to two group policy objects that did not adequately comply with the IRS' approved set of security

settings. For example, on the 5 servers, we tested the configurations for 12 user rights[11] that we considered sensitive and found an average of 10 unapproved user rights. Lastly, one server failed to meet standards because it had a high-risk vulnerability, the lack of antivirus protection.

Some noncompliant settings in group policy objects can be attributed to human error by those implementing the settings. Other noncompliant settings were made because the Active Directory® Team purposely created settings it considered stronger than the IRS' approved settings or to enable the server to perform a specific function. In both cases, changes to the settings were made without obtaining concurrence from the Chief, Mission Assurance and Security Services, and approval from the system owner, as required. We also noted written instructions for building and configuring Windows 2003® servers had not been prepared by the End User Equipment and Services organization before the servers were put into operation. These instructions may have improved the compliance rate of the settings used for the servers.

The use of unapproved security settings may create vulnerabilities for hackers or disgruntled employees to exploit. At a minimum, system administrators using unapproved settings diminish the capability of Active Directory® to ensure approved security controls are consistently implemented throughout the IRS network.

Sufficient oversight was not provided over system administrator accounts and access rights

The IRS requires employees to be provided only the access rights they need to carry out their responsibilities. System administrator accounts are especially powerful. Employees assigned to these accounts can make changes to the directory service, control directory-wide security settings, and install software. We found that, during the transition to Active Directory®, system administrator access was not adequately controlled, unnecessary system administrator accounts were established on servers, and built-in system administrator accounts were not being adequately safeguarded.

System administrator access was not adequately controlled. Industry best practices recommend keeping the membership of system administrator groups to the absolute minimum necessary to support the organization and limiting system administrator rights to only those needed by the individuals in the groups. Prior to implementation of Active Directory®, employees who may have needed only limited system administrator rights to carry out their responsibilities were assigned to system administrator groups with full system administrator capabilities because the previous operating system could not customize system administrator groups. For example, during a recent audit we found that employees were given full system administrator rights on

[11] User rights are tasks a user is permitted to perform on a computer or network. User rights determine who can log on to a system and the tasks they are permitted to perform. For example, a user can be given the right to change a system's time or access a system's security logs.

34 percent of the computers we tested just to obtain certain needed system administrator rights.[12] Active Directory® offers improved controls by creating system administrator groups whose rights can be customized to the needs of the employees in the groups.

During this review, the IRS began to create system administrator groups whose rights were customized. For example, a group was created with full system administrator rights, but the employees in the group could access only computers they were assigned to manage. Another group was created with limited system administrator rights to manage user accounts throughout the domain. The IRS is still developing criteria for granting system administrator access into Active Directory® based on the employees' job roles and determining approval paths for the various levels of access.

The process of reviewing and revising old rights and the establishment of centrally managed system administrator groups are expected to be a multiyear project and require buy-in from the various IRS business units. To expedite the implementation of Active Directory®, the IRS decided to use the same access rights (including system administrator rights) from the previous operating system regardless of whether the employees still needed all the rights in their groups. However, the risk of an employee accidentally or inappropriately accessing data or disrupting computer operations will be elevated until customized system administrator groups are established that limit users to only the rights they need.

Unnecessary system administrator accounts were established on servers. The IRS requires system administrator accounts to be created in centrally managed groups rather than on individual servers. Creating system administrator accounts on servers poses two problems. First, controls over accounts created on servers may be weaker than controls on accounts created centrally. Accounts on servers are governed by control settings on the servers, whereas accounts created in centrally controlled groups are governed by group policy objects. Because it is much more difficult to maintain consistent settings on individual servers than in group policy objects, the risk of security weaknesses increases. Second, finding and deleting accounts on servers for employees who change positions or leave the IRS can be a nearly impossible task in a large network because each server has to be checked. As a result, accounts that should be deleted may be overlooked and can be targeted for misuse by persons attempting to gain unauthorized access to the system. When accounts are created in a centrally controlled group, the group account is placed on the servers the group needs to access. When an employee no longer needs access to the servers, the employee just has to be removed from the central group.

We found system administrators had established system administrator accounts on 26 (49 percent) of the 53 servers we sampled. Sixty-eight system administrator accounts belonging to 27 system administrators had been directly created on these servers. Some of the accounts had been needed temporarily, while the servers were being prepared to be migrated into

[12] *Secure Configurations Are Initially Established on Employee Computers, but Enhancements Could Ensure Security Is Strengthened After Implementation* (Reference Number 2006-20-031, dated February 2006).

the Active Directory®-based network, but were not subsequently removed. Five (18.5 percent) of the 27 system administrators also had duplicate system administrator accounts that had been centrally created. As a result, the risk that system administrator accounts could be misused was increased.

Built-in system administrator accounts are not being adequately safeguarded. Every server is provided a built-in system administrator account named *Administrator* that was created as part of Microsoft's design of the operating system. Its purpose is to have an account that can be used if problems prevent system administrators from using their centrally created accounts. To prevent unauthorized persons from recognizing and using these accounts, the IRS requires system administrators to rename the accounts.

On 30 (57 percent) of the 53 servers we reviewed, system administrators had not sufficiently disguised the built-in accounts. The new names on the 30 servers still allowed these accounts to be identified as regular system administrator accounts. Even if the new names had fully disguised the accounts, the built-in system administrator accounts were readily apparent on all 53 sampled servers because, directly next to the account names, there were descriptions labeling them as built-in system administrator accounts. To fully disguise these powerful accounts, the descriptions should also be changed. Because these powerful accounts, unlike regular system administrator accounts, do not lock up after several unsuccessful attempts are made to guess the password, they could be the target of persons who are attempting to gain unauthorized access to the system or disrupt computer operations.

For the latter two issues, the Chief Information Officer has not provided sufficient oversight over system administrators to ensure they comply with procedures and best practices during the transition to Active Directory®. We are confident the Infrastructure Executive Steering Committee will provide the oversight and direction necessary to ensure consistent standards for administrative access are applied as soon as possible.

Recommendations

The Chief Information Officer should:

Recommendation 1: Formalize the approval process for distributing security settings in Active Directory® and ensure IRS standards are met. If deviations are suggested, concurrence from the Chief, Mission Assurance and Security Services, and approval from the system owner should be obtained.

> ***Management's Response:*** IRS management agreed with this recommendation. The Associate Chief Information Officer, End User Equipment and Services, will formalize the approval process for distributing security settings to Active Directory® using the policies and procedures currently in place for current systems and applications. Requests

for deviations will include the recommendation from the Chief, Mission Assurance and Security Services, and approval from the system owner.

Recommendation 2: Increase oversight of system administrator accounts and access rights during the transition to Active Directory®, enforce the IRS procedures that prohibit the creation of system administrator accounts on individual servers and require built-in system administrator accounts to be properly disguised, and periodically monitor computers for compliance and hold system administrators accountable for complying with these procedures.

Management's Response: IRS management agreed with this recommendation. The Associate Chief Information Officer, End User Equipment and Services, will increase and improve oversight of system administrator accounts during the transition to Active Directory® and review employees with Active Directory® system administrator rights. The Associate Chief Information Officer, End User Equipment and Services, will also enforce prohibitions on the system administrator accounts on individual servers, require built-in system administrator accounts to be properly disguised, monitor computers monthly for compliance, and hold system administrators accountable for complying with requirements.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether the Internal Revenue Service (IRS) had effectively and securely implemented the Active Directory®-based network and the Windows 2003® Server Operating System. To accomplish this objective, we:

I. Determined whether the IRS had effectively and securely created and implemented the structural components of Windows 2003® and Active Directory®.

A. Evaluated whether the forest,[1] domain,[2] and other structural components of Active Directory® were created and implemented soundly and securely following industry best practices.

B. Reviewed the adequacy of general security controls used to connect to and access Active Directory®.

C. Determined whether Active Directory® system administrators had received adequate training.

D. Reviewed the progress and status of Active Directory® features the IRS had not yet implemented.

E. Reviewed the progress and status of computing resources the IRS had not yet brought into the Active Directory®-based network.

II. Determined whether computers residing in the Active Directory®-based network were configured with strong security settings.

A. Reviewed the IRS' security standards to determine whether all computer security controls had been addressed.

B. Evaluated the procedures and methods the IRS uses to install security settings onto computers and test computers for compliance with security standards.

C. Selected a judgmental sample of 53 servers from the universe of 399 servers the IRS had moved into the Active Directory®-based network when we initiated this review in July 2005. We tested the 53 servers to determine whether strong computer security controls had been implemented through Active Directory®. Since servers with different server roles (for example, file servers, print servers, and domain controller

[1] The forest is the outermost logical boundary of Active Directory®.
[2] A domain is a group of computers on a network that are administered as a unit with common rules and procedures.

servers) have different security configurations, we judgmentally selected about 5 servers from each of the 12 server roles. Some server roles had a population of fewer than five servers. Judgmental samples were used because we were not planning to project the results against the entire universe.

D. Used the IRS' configuration-checking computer program to assess the adequacy of computer-based controls on the 53 sampled servers.

E. Reviewed the purpose, necessity, and security of groups and accounts that had been created directly on the 53 sampled servers.

III. Determined whether the IRS had effectively used organizational units and group policy objects[3] to ensure its computers met computer security standards.

A. Reviewed documentation on the IRS' organizational units and group policy objects.

B. Analyzed security weakness identified in the 53 sampled servers and determined whether group policy objects had been correctly configured.

C. Assessed the IRS' plans for continued progress in implementing organizational units and group policy objects.

[3] Group policy objects contain security settings which are applied to corresponding groups of computers.

Appendix II

Major Contributors to This Report

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)
Steve Mullins, Director
Gerald Horn, Audit Manager
Myron Gulley, Acting Audit Manager
Richard Borst, Senior Auditor
Mary Jankowski, Senior Auditor
Jody Kitazono, Senior Auditor
Stasha Smith, Senior Auditor

Appendix III

Report Distribution List

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

Appendix IV

Management's Response to the Draft Report

CHIEF INFORMATION OFFICER

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

RECEIVED
APR 17 2006

April 17, 2006

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: W. Todd Grams
Chief Information Officer

SUBJECT: Management Response to Draft Audit Report – The Enterprise-Wide Implementation of Active Directory Needs Increased Oversight (Audit #200520010) **(i-trak #2006-09372)**

Thank you for the opportunity to review the subject report and respond to the recommendations. We have carefully reviewed the report and agree that the recommendations have merit and require corrective action by the Internal Revenue Service (IRS).

Following the methodology that the Modernization and Information Technology Services (MITS) organization established for prioritizing corrective actions, we believe the recommendations in this audit are medium risk security issues.

As you note in your report, we established the Active Directory Tiger Team to provide the level of oversight needed to ensure the successful implementation of Active Directory, which includes ensuring the infrastructure architecture is agreed upon and IRS standards are met. In addition, prior to this audit, we established an Access Controls Project Team to clean-up access control irregularities, including those that migrated to Active Directory from the Windows NT network. The access controls action will prohibit the creation of system administrator accounts on individual servers and ensure required built-in system administrator accounts are properly disguised. It will also monitor the clean-up of administrative groups that are no longer necessary for systems administration.

We agree significant risks remain that must be addressed for the IRS to achieve the benefits of Active Directory. Hence, we are committed to improving the administration and security of the IRS Intranet. Our responses to the recommendations in this report are attached.

If you have questions, please call me at (202) 622-6800, or members of your staff may contact Judith Mills, Director, Program Oversight Office, at (202) 283-4915.

Attachment

Attachment

Draft Report – The Enterprise-Wide Implementation of Active Directory Needs Increased Oversight – Audit #200520010

RECOMMENDATION #1: The Chief Information Officer should formalize the approval process for distributing security settings in Active Directory and ensure IRS standards are met. If deviations are suggested, concurrence from the Chief of Mission Assurance and Security Services (MA&SS), and approval from the system owner should be obtained.

CORRECTIVE ACTION #1: We agree with this recommendation. The CIO will ensure that current policies and procedures that pertain to the approval process for distributing security settings for current systems and applications will also apply to Active Directory. The ACIO of End User Equipment and Services (EUES) will formalize the approval process and communicate this requirement to system and application owners. Requests for deviations will be made to the Chief of Data Security Operations who will assume responsibility for obtaining MA&SS' recommendation regarding the requested deviation. The Chief of Data Security Operations will forward MA&SS' recommendation to the system owner and obtain the system owner's approval.

IMPLEMENTATION DATE: January 2, 2007

RESPONSIBLE OFFICIAL: ACIO of End User Equipment and Services

CORRECTIVE ACTION MONITORING PLAN: Data Security Operations (DSO) staff will monitor the implementation of this corrective action and assume responsibility for obtaining approvals on deviation requests.

RECOMMENDATION #2: The Chief Information Officer should increase oversight of system administrator accounts and access rights during the transition to Active Directory; enforce the IRS' procedures that prohibit the creation of system administrator accounts to be properly disguised; and periodically monitor computers for compliance and hold system administrators accountable for complying with these procedures.

CORRECTIVE ACTION #2: We agree with this recommendation. EUES will increase and improve the oversight of system administrator accounts and access rights during the transition to Active Directory. The ACIO of EUES will communicate to the business units that EUES will conduct a review of all employees with Active Directory administrator rights. EUES will enforce the IRS' procedures that prohibit the creation of system administrator accounts on individual servers and require built-in system administrator accounts to be properly disguised. EUES will also monitor computers monthly for compliance and hold system administrators accountable for complying with these procedures.

IMPLEMENTATION DATE: January 2, 2007

Draft Report – The Enterprise-Wide Implementation of Active Directory Needs Increased Oversight – Audit #200520010

RESPONSIBLE OFFICIAL: ACIO of End User Equipment and Services

CORRECTIVE ACTION MONITORING PLAN: The Data Security Operations (DSO) staff will monitor the clean-up of administrative groups. They will conduct monthly employee reviews to ensure systems administrators are in compliance with security procedures related to accounts. On a continuing basis, the DSO Staff of EUES will coordinate with the Active Directory Tiger Team, MA&SS, and other components of MITS to ensure Active Directory administrative accounts comply with IRS security standards.