TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Progress Has Been Made in Using the Tivoli® Software Suite, Although Enhancements Are Needed to Better Distribute Software Updates and Reconcile Computer Inventories

December 2005

Reference Number: 2006-20-021

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

December 14, 2005

MEMORANDUM FOR CHIEF INFORMATION OFFICER

Michael R. Phillips

FROM: Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Progress Has Been Made in Using the Tivoli® Software Suite, Although Enhancements Are Needed to Better Distribute Software Updates and Reconcile Computer Inventories (Audit # 200520003)

This report presents the results of our review of the effectiveness of the Internal Revenue Service’s (IRS) Tivoli®[1] Enterprise Systems Management function applications. The Tivoli® applications provide the IRS with the ability to systemically deliver the most current versions of software and updated security patches[2] to employees’ computers and to scan the network for maintaining accurate computer inventory records. Because the IRS has over 100,000 employees, these tasks can be daunting; yet they are very important. Unsuccessful software distributions can lead to missing patches on computers, which, in turn, could expose the computers to exploitation by hackers, disgruntled employees, and/or malicious programs. In addition, maintaining an accurate computer inventory is crucial for the accuracy of the IRS’ financial statements.

Synopsis

The IRS has shown significant progress in using Tivoli® applications for distributing software updates to computers. Much of that progress can be attributed to the IRS’ efforts to improve Tivoli’s® ability to connect to more computers. While these improvements are commendable, the IRS can take further actions to improve its software distribution success rate, better use Tivoli® data for inventory reconciliation and software license management, and increase its overall ability to connect to computers.

[1] Tivoli® is a registered trademark owned by IBM.
[2] A patch is a fix to a program as a result of a design flaw in the program. Patches must be installed or applied to the applicable computer to correct the flaw.

The IRS has used Tivoli® to successfully install software updates to 77 percent of its computers, compared to 44 percent about 2 years ago. However, the two most frequent and important types of software distributions made (updates to the IRS' Common Operating Environment[3] and Microsoft Windows security patches) were also the most problematic during January through May 2005. The IRS installed only 62 percent of these software distributions successfully. In some instances, the IRS combined multiple updates into single distributions. We believe the size of the distributions made installation more difficult. We noted that the IRS lacks guidance on developing software distribution packages.

We also identified two inventory management issues that could be improved by using the Tivoli® software Inventory application. First, Tivoli® produces weekly reports to reconcile its data and data from the IRS' official computer equipment database, the Information Technology Asset Management System (ITAMS). We found these reconciliation reports identified an average of over 8,300 mismatched computers during the period March through May 2005. IRS personnel attempted to resolve the mismatched computers but were hampered by the mislabeling of computer names on the ITAMS. As such, the IRS abandoned these efforts. Because the mismatches were not resolved, the IRS' information technology inventory system likely does not include all IRS computers.

Second, the IRS did not use information from Tivoli® to ensure software installed on computers complied with license agreements. Tivoli® can aid in this effort through its ability to scan and identify software on every desktop and laptop computer, a process that, if done manually, would require an enormous effort. Tivoli® software data are not used because the IRS has not outlined policies and procedures regarding software management. By not managing software installations and licenses, the IRS could be violating software license agreements by installing more copies of software than were purchased, resulting in embarrassment and unnecessary legal fees. For example, Tivoli® data showed that 494 unique computers had proprietary reporting software installed, but the IRS could document only 142 licenses.

Lastly, the IRS estimates that Tivoli® can now connect to 95 percent of its computers, compared to 60 percent about 2 years ago. The ability to connect to more computers can have a direct effect on the success of software distributions and the accuracy of inventory management data. The IRS determines the percentage of computers managed by Tivoli® by whether Tivoli® has connected to a computer within 30 days. However, as recent events such as the Sasser worm[4] and other fast-moving computer security outbreaks have shown, the IRS must install critical security patches as soon as possible. We believe using a 1-week connectivity criterion is more

[3] The Common Operating Environment is a standardized, configured computer image integrated with a set of standard software packages to support the needs of all IRS employees.

[4] The Sasser worm exploited a flaw in the Local Security Authority Subservice System on Microsoft Windows computers and transferred additional exploitable code to the computers. It also probed for other computers to infect. This worm rendered computers inoperable.

realistic and appropriate in today's environment. Using this criterion, we estimate the IRS cannot reach 18 percent of its computers (approximately 18,750 computers) in any given week.

We identified several reasons why some computers cannot connect to the Tivoli® system or did not have the Tivoli® client software installed. For example, the IRS had not documented procedures for installing and maintaining Tivoli® software on computers, responsible persons did not have access to computers to resolve connection problems, and the IRS may have taken some computers out of service without notifying employees responsible for maintaining Tivoli® applications. By being unable to connect to thousands of computers through the Tivoli® system, the IRS will not be fully benefiting from the use of Tivoli® and will continue to use limited resources to manually administer these computers, particularly for installing the latest virus patches and inventorying hardware and software.

Recommendations

To improve software distributions, we recommended the Chief Information Officer develop procedures that provide formal guidance and standardization in preparing software distributions.

To improve the use of Tivoli® software Inventory application data, we recommended the Chief Information Officer require the Associate Chief Information Officer, End User Equipment and Services, to resolve mismatches between Tivoli® data and the ITAMS and to ensure all desktops, laptops, and servers comply with the IRS' computer naming standards. The Chief Information Officer should ensure software management policies and procedures are provided and responsibility for software management is specified. The policies and procedures should require the use of Tivoli® software Inventory application data to monitor compliance with software licenses.

To improve Tivoli® computer connectivity, we recommended the Chief Information Officer notify all employees of the need for computers to remain online whenever possible, provide employees assigned Tivoli® responsibilities adequate access to computers, separately account for Tivoli® computers that are taken out of service for backup or emergency purposes, and assign formal responsibility for incorporating computers without the Tivoli® client software into Tivoli®.

Response

IRS management agreed with all of our recommendations. Specifically, the Associate Chief Information Officer, End User Equipment and Services, will develop formal procedures that provide guidance and standardization in the preparation of software distributions; develop procedures to resolve mismatches between Tivoli® data and the ITAMS, ensuring all desktops, laptops, and servers comply with the IRS' computer naming standards; and develop software management policies and procedures that will identify responsibility for software management.

These procedures will require the use of Tivoli® software Inventory application data to monitor compliance with software licenses.

The Associate Chief Information Officer, End User Equipment and Services, will also develop a plan and procedures to ensure appropriate Enterprise Systems Management function employees have adequate access to computers and networks to resolve computer connectivity issues. The plan and procedures will account for modifying the script[5] used for installing the Tivoli® software client on users' workstations via the Windows Administration group for the purpose of managing Tivoli® computers. Second, the plan and/or procedures will also grant access to appropriate personnel in the Offices of Appeals, Chief Counsel, and Criminal Investigation for managing Tivoli® computer connections.

In addition, the Associate Information Officer, End User Equipment and Services, will continue to notify all IRS employees via Employee Advisories of the need for computers to remain online and connected to the IRS network whenever possible; develop appropriate processes and procedures to provide exception reporting when computers are taken offline and brought back online to ensure Tivoli® recognizes them; and develop a process/procedure to identify systems that are not being managed by Tivoli® software so they can either receive the Tivoli® software, become part of the Tivoli® managed group, or be removed from the network. Management's complete response to the draft report is included as Appendix IV.

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 Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

[5] A script is a short program written in general-purpose programming language to perform certain tasks, including those that are repetitive in nature.

Table of Contents

Background

The Internal Revenue Service (IRS) has over 100,000 employees, many of whom use a computer to carry out their job responsibilities. To address the challenge of managing and controlling its geographically dispersed computer resources, the IRS implemented the Tivoli®[1] software suite. The Tivoli® applications have the potential to improve productivity by systemically delivering the most current versions of software and updated security patches[2] to employees' computers.

Security patches are important in protecting an agency's computers from viruses and hackers. Typically, the software industry self-polices the quality of its products by identifying software security vulnerabilities after the product has been on the market. To correct these security vulnerabilities, the software vendors issue security patches. However, hackers are also acutely aware of all security vulnerabilities being identified and will use these vulnerabilities to launch attacks and/or create malicious programs to take advantage of these flaws.

The importance of installing security patches was best illustrated with a 2004 Federal Bureau of Investigation study,[3] which showed that 91 percent of all computer system intrusions could have been prevented if related security patches had been implemented for countering known vulnerabilities. The *2005 E-Crime Watch* survey[4] found that manual patch management, a method still commonly used, was rated as the single least effective technology used by organizations responding to the survey. Coupled with the fact that the CERT® Coordination Center[5] found 3,780 security vulnerabilities were reported during 2004, it is clear that manual patching in a large bureau like the IRS would be overwhelming and ineffective.

By using the Tivoli® software suite to perform the task of distributing software updates and security patches, the IRS can use its limited information technology personnel resources more efficiently. The Tivoli® software suite also provides the IRS with the ability to automatically scan and collect hardware and software information that can be used to improve the accuracy of

[1] Tivoli® is a registered trademark owned by IBM.
[2] A patch is a fix to a program as a result of a design flaw in the program. Patches must be installed or applied to the applicable computer to correct the flaw.
[3] The *2004 Computer Crime and Security Survey* was conducted by the Computer Security Institute with the participation of the San Francisco Federal Bureau of Investigation's Computer Intrusion Squad. The 2004 survey results were based on the responses of 494 computer security practitioners across the United States.
[4] This survey was conducted by *CSO* (Chief Security Officer) magazine in cooperation with the United States Secret Service and the Carnegie Mellon University Software Engineering Institute's CERT® Coordination Center. The research was conducted to unearth electronic crime-fighting trends and techniques, including best practices and emerging trends.
[5] Established in 1988, the CERT® Coordination Center is a center of Internet security expertise, located at the Software Engineering Institute, a Federally funded research and development center operated by Carnegie Mellon University.

the IRS computer inventory. This inventory is critical because it is used to support IRS financial statements. Use of a manual method would require the IRS computer support staff to physically log onto each computer, creating too great a burden due to the sheer number of computers maintained by the IRS.

Responsibility for using the Tivoli® software suite lies with the Enterprise Systems Management (ESM) function, whose mission is to provide design, development, deployment, and operational support for the enterprise-wide management of IRS computers. The ESM function is part of the End User Equipment and Services division of the Information Technology Services organization.

In Fiscal Year 2003, we conducted a review of the IRS' implementation of the Tivoli® software suite,[6] identifying several weaknesses in the management control practices that, if not corrected, could reduce the overall effectiveness and actual benefits of the Tivoli® implementation. The weaknesses included the absence of policies and guidelines to promote Tivoli® computer connectivity and a lack of staff assigned to resolve Tivoli® computer connectivity and software distribution problems.

While the IRS uses several Tivoli® applications, this review focused on the Tivoli® software Distribution and software Inventory applications. In addition, we reviewed the effectiveness of IRS efforts to improve Tivoli® computer connectivity, which is critical to the effectiveness of all Tivoli® applications. This review was performed in the Information Technology Services organization at the IRS National Headquarters in Washington, D.C., and the Austin Campus[7] in Austin, Texas, during the period December 2004 through May 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.

[6] *The Implementation of Software Products to Manage and Control Computer Resources Needs Improvement* (Reference Number 2003-20-151, dated July 2003).

[7] 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

Since our last review in this area, the IRS has used the Tivoli® software suite to improve software distribution to its computers, but some critical updates are not being installed. We also noted that the IRS could use Tivoli® data to better manage its computer inventory. The success of each of these tasks depends on the ability of the Tivoli® software to connect with computers across the IRS network. We found that the IRS has significantly improved the ability of the Tivoli® software to connect with computers; however, enhancements can be made.

While Software Distribution Has Improved, Critical Updates Were Not Always Installed

The IRS has shown significant progress with the Tivoli® software Distribution application since our last report. Most notably, the percentage of software distribution packages reaching targeted computers increased from 44 percent in April 2003 to 77 percent in May 2005.[8]

Despite the improvement, the IRS has experienced some problems with certain types of software distributions. From January through May 2005, software updates for the Common Operating Environment (COE)[9] and Microsoft patch updates, which were the two most frequent and important types of distributions made using the Tivoli® software Distribution application, were the most problematic. For these 2 types of distributions, the success rate was 62 percent, as illustrated in Table 1. Aside from these 2 types of distributions, the remaining 2,912 distributions during that time period had a success rate of 81 percent.

Tivoli® distributions for the COE and Microsoft products were the most problematic, having a success rate of 62 percent compared to 81 percent for all other distributions.

[8] The success rate is a snapshot from the ESM function's web site, as of May 2005, and represents all software distributions since the ESM function started tracking this information. The 77 percent was derived by dividing 3,720,342 successful distributions by the 4,808,624 total distribution attempts from July 2003 to May 2005.

[9] The COE is a standardized, configured computer image integrated with a set of standard software packages to support the needs of all IRS employees.

Table 1: Software Distributions for the COE and Microsoft Patches From January Through May 2005

Distribution Type	Number of Distributions	Number of Targets	Number of Successful Distributions	Success Rate
COE	533	480,546	259,550	54%
Microsoft Patches	915	725,303	484,091	67%
Totals	1,448	1,205,849	743,641	62%

Source: Software distribution data from the ESM function.

The COE distributions are important in maintaining current versions of software used by IRS employees. Microsoft patches are designed to maintain the performance and security of Windows-based computers and products. Further analysis of the Microsoft patches identified a wide variance in success. While some Microsoft patch distributions were very successful, such as one that successfully reached 86 percent of its 70,000 targets, many others reached fewer than 50 percent of their targets, as shown in Table 2.

Table 2: Microsoft Patch Distributions From January Through April 2005 That Were Less Than 50 Percent Successful

Date of Microsoft Patch Distribution	Number of Distributions	Number of Targets	Number of Successful Distributions	Success Rate
4/7/2005	27	142	26	18%
2/10/2005	11	966	285	30%
4/11/2005	19	18,868	6,057	32%
4/15/2005	20	37,778	14,853	39%
4/19/2005	6	13,353	5,995	45%
2/12/2005	44	39,543	18,700	47%

Source: Software distribution data from the ESM function.

Oversized update packages can cause software distributions to fail. According to ESM function personnel, both Microsoft patches and COE packages often include multiple updates, resulting in packages that may be too large to successfully install. For example, the Microsoft patch packages listed in Table 2 included multiple updates. The ultimate success of a multiple update distribution is contingent on success for all updates. If one update within the package fails, the entire distribution fails.

Although the IRS has informal procedures for software distribution, it has not adopted formal procedures. Without documented guidelines, large packages are developed that may not be delivered through the IRS' network, do not install properly, or incapacitate computers used to distribute the packages.

In addition, documented procedures could identify steps to follow in emergency situations. These procedures are critical if staff is unavailable to distribute critical software patches when new viruses emerge. For example, during the IRS response to the Sasser worm[10] in May 2004, existence of formal procedures may have averted an error in the distribution program that resulted in the spread of this worm. The Sasser worm penetrated the IRS network and resulted in an estimated $50 million in lost productivity due to the loss of connectivity caused by the worm.

One of the reasons for software distribution failures is the overly large sizes of the update packages. This condition stems from the lack of documented procedures to ensure packages are consistently prepared and developed.

Software distribution to IRS computers is critical to maintain optimal protection of computers and taxpayer data and to ensure the continued performance of computer operations. Unsuccessful distributions can lead to outdated software that affects productivity and to missing patches on computers, which, in turn, could expose the computer to exploit by hackers, disgruntled employees, and/or malicious programs.

Recommendation

Recommendation 1: The Chief Information Officer should develop formal procedures that provide guidance and standardization in the preparation of software distributions, including the bundling of multiple packages and steps for emergency situations.

> ***Management's Response:*** The Associate Chief Information Officer, End User Equipment and Services, will develop formal procedures that provide guidance and standardization in the preparation of software distributions. This guidance will include the bundling of multiple packages and steps for emergency situations.

Tivoli® Data Are Not Being Used to Manage Computer Inventory and Software Licenses

According to IRS policy, the Chief Information Officer is responsible for ownership, management, and control of all computer property in the IRS. The Information Technology

[10] The Sasser worm exploited a flaw in the Local Security Authority Subservice System on Microsoft Windows computers and transferred additional exploitable code to the computers. It also probed for other computers to infect. This worm rendered computers inoperable.

Asset Management System (ITAMS) is used to record all computer inventories. Tivoli® provides excellent information to supplement the ITAMS database. However, information from Tivoli® on computer equipment inventory and software installed on desktops and laptops has not been used effectively.

Mismatches between Tivoli® computer inventory data and the ITAMS are not being resolved

The Tivoli® software Inventory application provides current inventory data to the IRS' official computer equipment inventory database, the ITAMS. On a weekly basis, the Tivoli® software Inventory application performs an initial reconciliation between its records and inventory information from the ITAMS and produces reconciliation reports containing mismatched computer equipment. From March through May 2005, the number of computers that could not be reconciled averaged over 8,300 computers.

The End User Equipment and Services division had made initial attempts to resolve the mismatched computer equipment. However, these efforts were hampered by the mislabeling of computer names on the ITAMS. Because of these difficulties and because responsibility for reconciling the reports had not been formally assigned, the End User Equipment and Services division abandoned its efforts to resolve mismatches.

Reconciliation reports between the Tivoli® software Inventory application and the ITAMS showed an average of over 8,300 mismatched computers.

Our assessment of inventory reconciliation reports from March through May 2005 determined computers that did not comply with the IRS' naming standards accounted for 36 percent of the computers identified by Tivoli® that were not listed on the ITAMS. These mislabeled computers may not contain information necessary to resolve the mismatch, such as location code, machine type, or computer bar code.

We also found that the remaining mismatched computers were mainly caused by the inability of the Tivoli® software to successfully connect to computers with and without the Tivoli® software client installed. This issue is discussed later in this report. When the mismatched computers are not resolved, the ITAMS does not include accurate hardware information for all IRS computers.

Additionally, incomplete inventory information on IRS computers affects the accuracy of the IRS' financial statements by causing them to have an inaccurate accounting of all IRS computer assets. Without an accurate accounting of computer assets, management does not have information needed to make purchasing decisions for new computer equipment.

Tivoli® software inventory data are not used

The Tivoli® software Inventory application has the ability to scan the Tivoli® computers to identify information on registered software and unknown application files on a frequent, often daily, basis. However, there is no indication these data are used to manage the IRS' software inventory on desktops and laptops. No formal requests for this information have been received by ESM function personnel, other than internal administrative requests. In addition, there is no capability to search for specific software information on the ESM function's web site.

The Tivoli® software Inventory application has the ability to identify both registered and unauthorized software. However, there is no indication these data are used to manage software inventory.

With over 100,000 IRS computers, the resources needed to manage compliance with software license agreements and identify unauthorized software are immense. The Government Accountability Office (GAO) has previously reported on the IRS' control weaknesses in managing software licenses and determining compliance with them.[11] The Tivoli® software Inventory application can aid in this effort since it can inventory the software on every desktop and laptop, a process that, if done manually, would require an enormous effort.

However, we found the IRS has not provided specific procedures for using the Tivoli® software Inventory application to monitor compliance with existing software licenses. While the IRS' asset management procedures include a title on software management, the section is blank and reserved for later use.

By not managing software installations and licenses, the IRS may install more copies of the software than were purchased. As a result, the IRS could be violating software license agreements, which could result in embarrassment and unnecessary legal fees. As an example, the IRS analyzed the use of the Monarch software products[12] using data from Tivoli®, the ITAMS, and other sources. In the analysis, the IRS provided documentation for 142 Monarch software licenses. The IRS had also purchased an indeterminate number of licenses for a Monarch software product for which documentation did not exist. The Tivoli® data showed that 494 unique computers had a Monarch product installed. When this information was compared against the software license data for the Monarch products, the IRS determined the number of software installations far exceeded the number of licenses purchased.

[11] *Financial Audit: IRS's Fiscal Year 2001 and 2000 Financial Statements* (GAO-02-414, dated February 2002).

[12] Monarch is proprietary software used to create, analyze, and read Collection Activity Reports.

Recommendations

The Chief Information Officer should:

Recommendation 2: Require the Associate Chief Information Officer, End User Equipment and Services, to resolve mismatches between Tivoli® data and the ITAMS and to ensure all desktops, laptops, and servers comply with the IRS' computer naming standards.

> ***Management's Response:*** The Associate Chief Information Officer, End User Equipment and Services, will develop appropriate procedures to resolve mismatches between Tivoli® data and the ITAMS, ensuring all desktops, laptops, and servers comply with the IRS' computer naming standards.

Recommendation 3: Ensure software management policies and procedures are provided and responsibility for software management is specified. The policies and procedures should require the use of Tivoli® software Inventory application data to monitor compliance with software licenses.

> ***Management's Response:*** The Associate Chief Information Officer, End User Equipment and Services, will develop software management policies and procedures. The policies and procedures will identify responsibility for software management and will require the use of Tivoli® software Inventory application data to monitor compliance with software licenses.

Tivoli® Could Improve Software Distribution and Inventory Management by Connecting to More Computers

The effectiveness of all Tivoli® applications, including those for software distribution and inventory management, is dependent on the system's ability to successfully communicate with computers on the IRS network. Before the Tivoli® system can connect to an IRS computer, the Tivoli® client software must be properly installed.[13]

The IRS has significantly improved Tivoli's® ability to connect to computers since our July 2003 report. In that report, we found the IRS had a computer connectivity rate of 60 percent (78,925 of 131,488 computers) in April 2003. The IRS estimates it reached an average of 95 percent (98,545 of 104,147 computers) from January through April 2005. These improvements were largely due to the use of comprehensive Tivoli® procedures established since our last review.

[13] Tivoli® terminology refers to computer connectivity as "endpoint health." A computer that can communicate with the Tivoli® servers is considered a "healthy endpoint," whereas a computer that had once communicated with the Tivoli® server but is no longer able to is called an "unhealthy endpoint."

While this improvement is commendable, we are concerned with the IRS' ability to quickly reach its computers when the need arises. The IRS determines its computer connectivity percentage on whether Tivoli® has connected to a computer within the last 30 days. However, as recent events such as the Sasser worm and other fast-moving computer security outbreaks have shown, the IRS must install critical security patches as soon as possible. As such, we believe the 30-day criterion is not realistic and using a 1-week connectivity criterion is more appropriate in today's environment. Factoring in computers without the Tivoli® client software and our 1-week criterion, we estimate the IRS cannot reach 18 percent of its computers, or approximately 18,750 computers, in any given week.

We estimate the IRS cannot reach 18 percent of its computers, or approximately 18,750 computers, in any given week.

Aside from the change in connection criterion, there are several reasons why some computers cannot successfully connect to the Tivoli® system or did not have the Tivoli® client software installed. The following areas of concern are based on either our analyses of Tivoli® data or interviews with ESM function team members responsible for the Tivoli® applications:

- The installation and maintenance of the Tivoli® client software were inconsistently performed, mainly due to undocumented procedures. For example, the Tivoli® client software should be installed through a script[14] after the COE has been installed. However, different versions of the script are used, or, in some cases, no script is used at all.
- ESM function employees were not always given adequate access, through the Windows Administration group, to desktop and laptop computers to restore their connectivity. This group was not added as part of the script used to install Tivoli® client software after the COE has been installed. In addition, they did not have access to restricted networks used by several IRS functions, including those used by the Offices of Appeals, Chief Counsel, and Criminal Investigation. Without access to these networks, the team is dependent on these other functions to maintain computer connectivity, which may not be their highest priority.
- The IRS has computers that were once on the network but have since been taken out of service for long periods of time. These computers include those that are inadvertently turned off and those taken out of service for future backup or emergency use. When ESM function employees are not notified of these computers, the Tivoli® system will continue to show these computers as being in service but will be unable to connect with them.

[14] A script is a short program written in general-purpose programming language to perform certain tasks, including those that are repetitive in nature.

- Neither the ESM function nor the End User Equipment and Services division has been formally assigned the responsibility for ensuring all computers are brought into the Tivoli® system, which includes installing the Tivoli® client software on users' computers. Complicating this effort is the large number of computers that are no longer active on the IRS network. The ESM function program[15] used to identify computers without the Tivoli® client software does so by scanning the IRS' Windows Domain servers but does not distinguish between active and inactive accounts.

By being unable to connect to thousands of computers through the Tivoli® system, the IRS will continue to rely on limited staffing to manually administer these computers, particularly for installing the latest security patches and inventorying hardware and software. Consequently, the risk of one or more of these computers being vulnerable to viruses, worms, and other attacks remains high. Also, the IRS could understate its financial statements by being unable to verify its inventory of computer systems through Tivoli® software Inventory application scans.

Recommendations

The Chief Information Officer should:

Recommendation 4: Ensure appropriate ESM function employees have adequate access to computers and networks to resolve computer connectivity problems. First, the script used for installing the Tivoli® software client on users' computers should be modified to allow access by ESM function employees via the Windows Administration group to manage Tivoli® computers. Second, access to restricted networks, such as those in the Offices of Appeals, Chief Counsel, and Criminal Investigation, should be granted to personnel responsible for managing Tivoli® computer connections.

> ***Management's Response:*** The Associate Chief Information Officer, End User Equipment and Services, will develop a plan and procedures to ensure appropriate ESM function employees have adequate access to computers and networks to resolve computer connectivity issues. The plan and procedures will also account for modifying the script used for installing the Tivoli® software client on users' workstations via the Windows Administration group for the purpose of managing Tivoli® computers. Second, the plan and/or procedures will also grant access to appropriate personnel in the Offices of Appeals, Chief Counsel, and Criminal Investigation for managing Tivoli® computer connections.

Recommendation 5: Notify all IRS employees of the need for computers to remain online and connected to the IRS network whenever possible so Tivoli® can communicate with them and perform management functions.

[15] ESM function personnel developed the E-Touch program to supplement data from Tivoli® and assist in identifying computers without the Tivoli® client software.

> ***Management's Response:*** The Associate Chief Information Officer, End User Equipment and Services, will continue to notify all IRS employees via Employee Advisories of the need for computers to remain online and connected to the IRS network whenever possible.

Recommendation 6: Separately account for Tivoli® computers that are taken out of service for backup or emergency purposes. When these computers are brought back online, Tivoli® should recognize them as active.

> ***Management's Response:*** The Associate Chief Information Officer, End User Equipment and Services, will develop appropriate processes and procedures to provide exception reporting when computers are taken offline and brought back online to ensure Tivoli® recognizes them.

Recommendation 7: Assign formal responsibility for using data available from the ITAMS or other sources to identify active computers on the IRS network that do not have the Tivoli® client software installed and for ensuring those computers have the Tivoli® software and can successfully connect with the Tivoli® system.

> ***Management's Response:*** The Associate Chief Information Officer, End User Equipment and Services, will develop a process/procedure to identify systems that are not being managed by Tivoli® software so they can either receive the Tivoli® software, become part of the Tivoli® managed group, or be removed from the network.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to assess the effectiveness of the Internal Revenue Service's (IRS) Tivoli®[1] Enterprise Systems Management (ESM) function applications. While the IRS has several Tivoli® applications, this review focused on the Tivoli® software Distribution and software Inventory applications. In addition, we reviewed the effectiveness of the IRS' efforts to improve Tivoli® computer connectivity, which is critical to the effectiveness of all Tivoli® applications. To accomplish this objective, we:

I. Determined whether computer connectivity was adequately managed.

A. Identified policies, procedures, and standards for managing Tivoli® computer connections.

B. Assessed the process for managing computer connectivity. We extracted computer connection data from the ESM function's web site for each week from January 19 to April 28, 2005. These data included information on all IRS Tivoli®-enabled computers (the highest total being 105,424 during the time period) and E-touch systems[2] (the highest total being 10,845 during the time period).

C. Identified factors limiting the success of Tivoli® computer connectivity, including interviewing all seven Tivoli® team members and identifying trends from Tivoli® data obtained.

II. Assessed the effectiveness of patch[3] management and software updates using the Tivoli® software Distribution application.

A. Identified policies, procedures, and standards for patch management and software updates.

B. Assessed the process for patch management and software update using Tivoli®.

C. Assessed the impact of incomplete patching and incomplete software updates of IRS computers. We obtained a detailed summary of all IRS enterprise-wide software distributions for Calendar Year 2005. This included data for all 4,360 distributions

[1] Tivoli® is a registered trademark owned by IBM.

[2] The E-Touch program is a supplemental program developed by ESM function personnel to assist in identifying computers in the IRS' architecture, particularly those outside of the Tivoli® environment.

[3] A patch is a fix to a program as a result of a design flaw in the program. Patches must be installed or applied to the applicable computer to correct the flaw.

made through May 6, 2005. These data included the package type, size, and date of distribution.

D. Identified factors limiting the success of patch management and software updates using Tivoli®.

III. Assessed the effectiveness of inventorying software and hardware using the Tivoli® software Inventory application.

A. Identified policies, procedures, and standards for inventorying hardware and software.

B. Assessed the process for inventorying software and hardware.

C. Assessed the impact of inadequate management of hardware and software inventory. We reviewed all nine available weekly Tivoli®/Information Technology Asset Management System (ITAMS) reconciliation reports available on the ESM function's web site from March through May 2005. These reports provide details on computers managed by Tivoli® but not found on the ITAMS and vice versa.

D. Identified factors limiting the success of software and hardware inventory.

IV. Assessed the effectiveness of managing software licenses using the Tivoli® software Inventory application.

A. Identified policies, procedures, and standards for managing software licenses.

B. Assessed the process for managing software licenses.

C. Assessed the impact of inadequate management of software licenses.

D. Identified factors limiting the success of software license management.

Appendix II

Major Contributors to This Report

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)
Stephen Mullins, Director
Kent Sagara, Audit Manager
Myron L. Gulley, Senior Auditor
Michael A. Howard, Senior Auditor
Jimmie Johnson, Senior Auditor
Anthony D. Knox, Senior Auditor

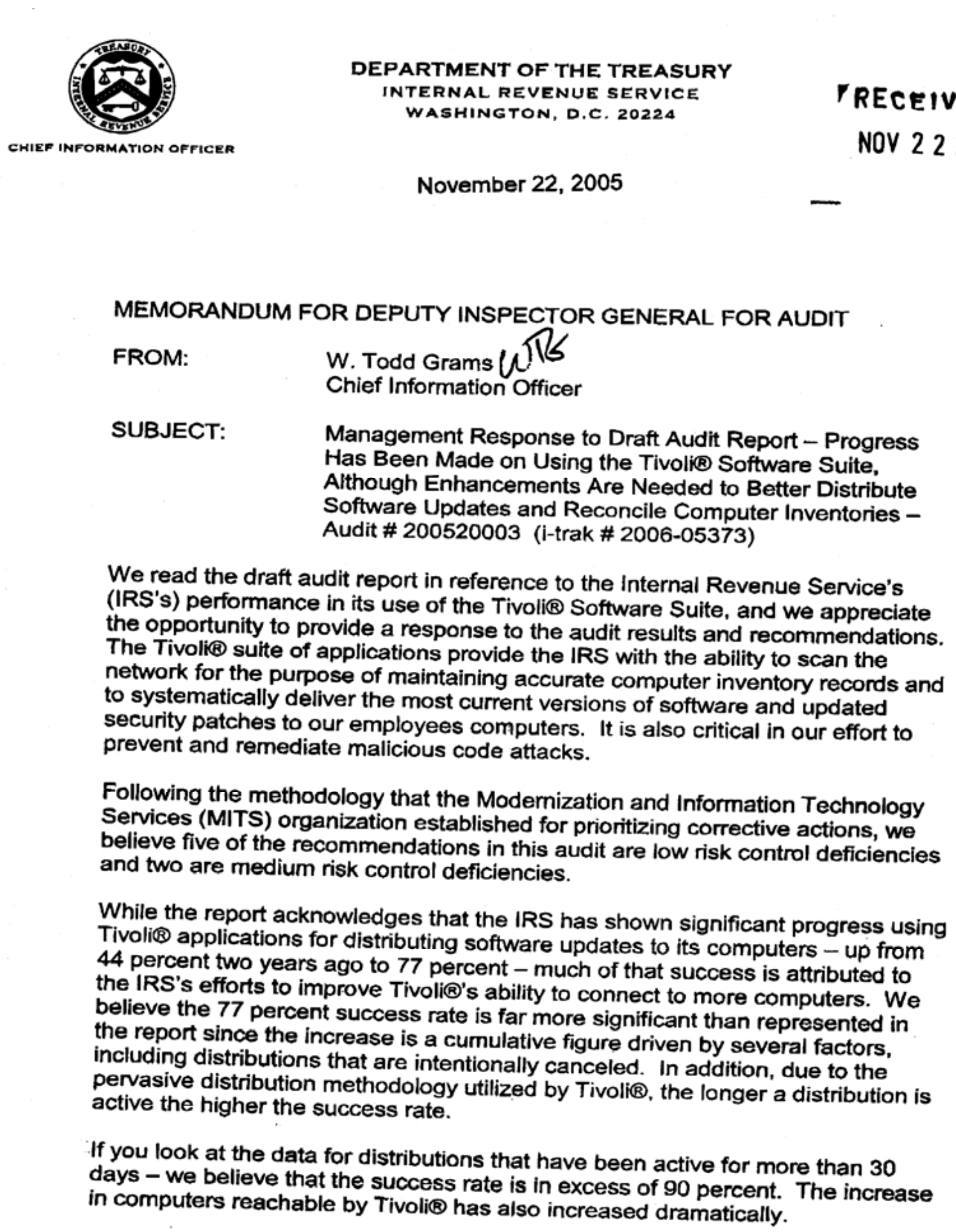
Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Associate Chief Information Officer, End User Equipment and Services OS:CIO:I:EU
Associate Chief Information Officer, Enterprise Networks OS:CIO:I:EN
Associate Chief Information Officer, Enterprise Operations Services OS:CIO:I:EO
Director, Enterprise Systems Management OS:CIO:I:EU:ESM
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 Liaison: Chief Information Officer OS:CIO

Appendix IV

Management's Response to the Draft Report



CHIEF INFORMATION OFFICER

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

November 22, 2005

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: W. Todd Grams WTG
Chief Information Officer

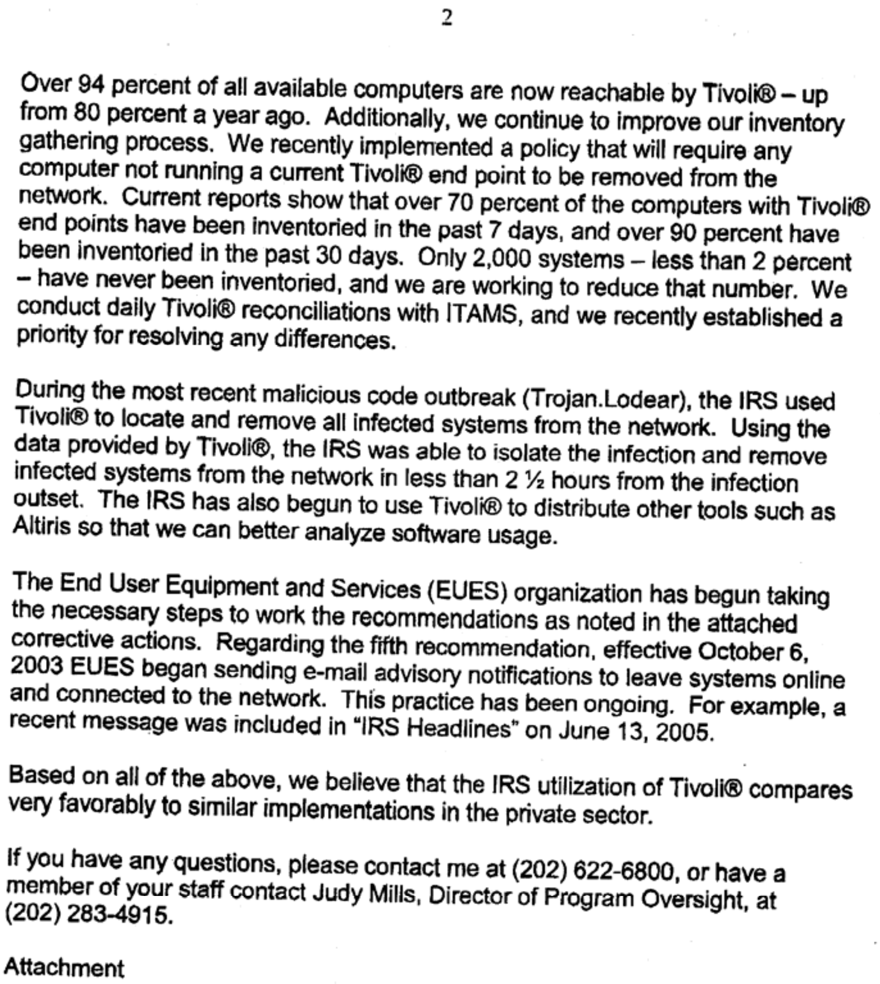
SUBJECT: Management Response to Draft Audit Report – Progress Has Been Made on Using the Tivoli® Software Suite, Although Enhancements Are Needed to Better Distribute Software Updates and Reconcile Computer Inventories – Audit # 200520003 (i-trak # 2006-05373)

We read the draft audit report in reference to the Internal Revenue Service's (IRS's) performance in its use of the Tivoli® Software Suite, and we appreciate the opportunity to provide a response to the audit results and recommendations. The Tivoli® suite of applications provide the IRS with the ability to scan the network for the purpose of maintaining accurate computer inventory records and to systematically deliver the most current versions of software and updated security patches to our employees computers. It is also critical in our effort to prevent and remediate malicious code attacks.

Following the methodology that the Modernization and Information Technology Services (MITS) organization established for prioritizing corrective actions, we believe five of the recommendations in this audit are low risk control deficiencies and two are medium risk control deficiencies.

While the report acknowledges that the IRS has shown significant progress using Tivoli® applications for distributing software updates to its computers – up from 44 percent two years ago to 77 percent – much of that success is attributed to the IRS's efforts to improve Tivoli®'s ability to connect to more computers. We believe the 77 percent success rate is far more significant than represented in the report since the increase is a cumulative figure driven by several factors, including distributions that are intentionally canceled. In addition, due to the pervasive distribution methodology utilized by Tivoli®, the longer a distribution is active the higher the success rate.

If you look at the data for distributions that have been active for more than 30 days – we believe that the success rate is in excess of 90 percent. The increase in computers reachable by Tivoli® has also increased dramatically.



Over 94 percent of all available computers are now reachable by Tivoli® – up from 80 percent a year ago. Additionally, we continue to improve our inventory gathering process. We recently implemented a policy that will require any computer not running a current Tivoli® end point to be removed from the network. Current reports show that over 70 percent of the computers with Tivoli® end points have been inventoried in the past 7 days, and over 90 percent have been inventoried in the past 30 days. Only 2,000 systems – less than 2 percent – have never been inventoried, and we are working to reduce that number. We conduct daily Tivoli® reconciliations with ITAMS, and we recently established a priority for resolving any differences.

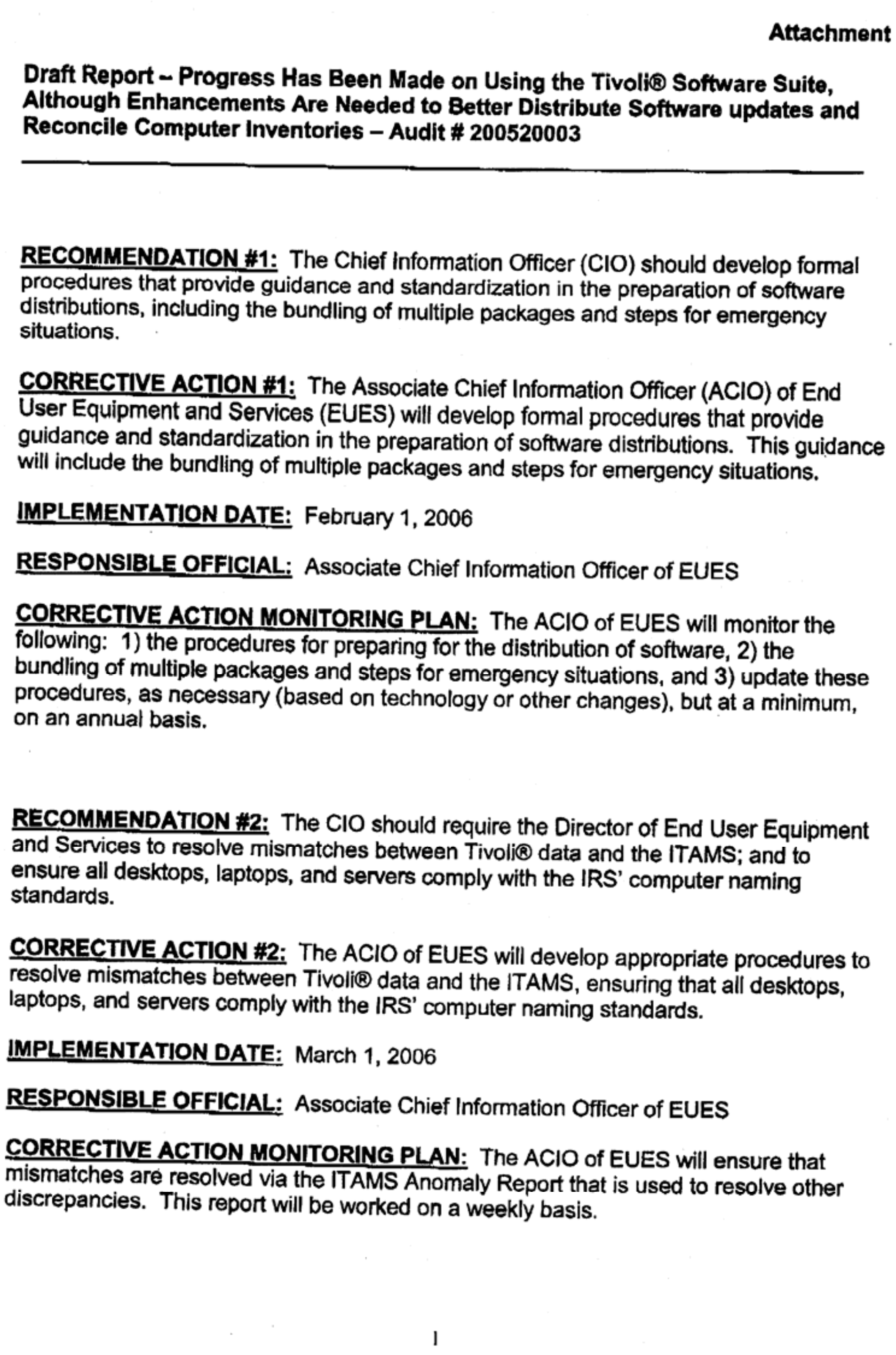
During the most recent malicious code outbreak (Trojan.Lodear), the IRS used Tivoli® to locate and remove all infected systems from the network. Using the data provided by Tivoli®, the IRS was able to isolate the infection and remove infected systems from the network in less than 2 ½ hours from the infection outset. The IRS has also begun to use Tivoli® to distribute other tools such as Altiris so that we can better analyze software usage.

The End User Equipment and Services (EUES) organization has begun taking the necessary steps to work the recommendations as noted in the attached corrective actions. Regarding the fifth recommendation, effective October 6, 2003 EUES began sending e-mail advisory notifications to leave systems online and connected to the network. This practice has been ongoing. For example, a recent message was included in "IRS Headlines" on June 13, 2005.

Based on all of the above, we believe that the IRS utilization of Tivoli® compares very favorably to similar implementations in the private sector.

If you have any questions, please contact me at (202) 622-6800, or have a member of your staff contact Judy Mills, Director of Program Oversight, at (202) 283-4915.

Attachment



Attachment

Draft Report – Progress Has Been Made on Using the Tivoli® Software Suite, Although Enhancements Are Needed to Better Distribute Software updates and Reconcile Computer Inventories – Audit # 200520003

RECOMMENDATION #1: The Chief Information Officer (CIO) should develop formal procedures that provide guidance and standardization in the preparation of software distributions, including the bundling of multiple packages and steps for emergency situations.

CORRECTIVE ACTION #1: The Associate Chief Information Officer (ACIO) of End User Equipment and Services (EUES) will develop formal procedures that provide guidance and standardization in the preparation of software distributions. This guidance will include the bundling of multiple packages and steps for emergency situations.

IMPLEMENTATION DATE: February 1, 2006

RESPONSIBLE OFFICIAL: Associate Chief Information Officer of EUES

CORRECTIVE ACTION MONITORING PLAN: The ACIO of EUES will monitor the following: 1) the procedures for preparing for the distribution of software, 2) the bundling of multiple packages and steps for emergency situations, and 3) update these procedures, as necessary (based on technology or other changes), but at a minimum, on an annual basis.

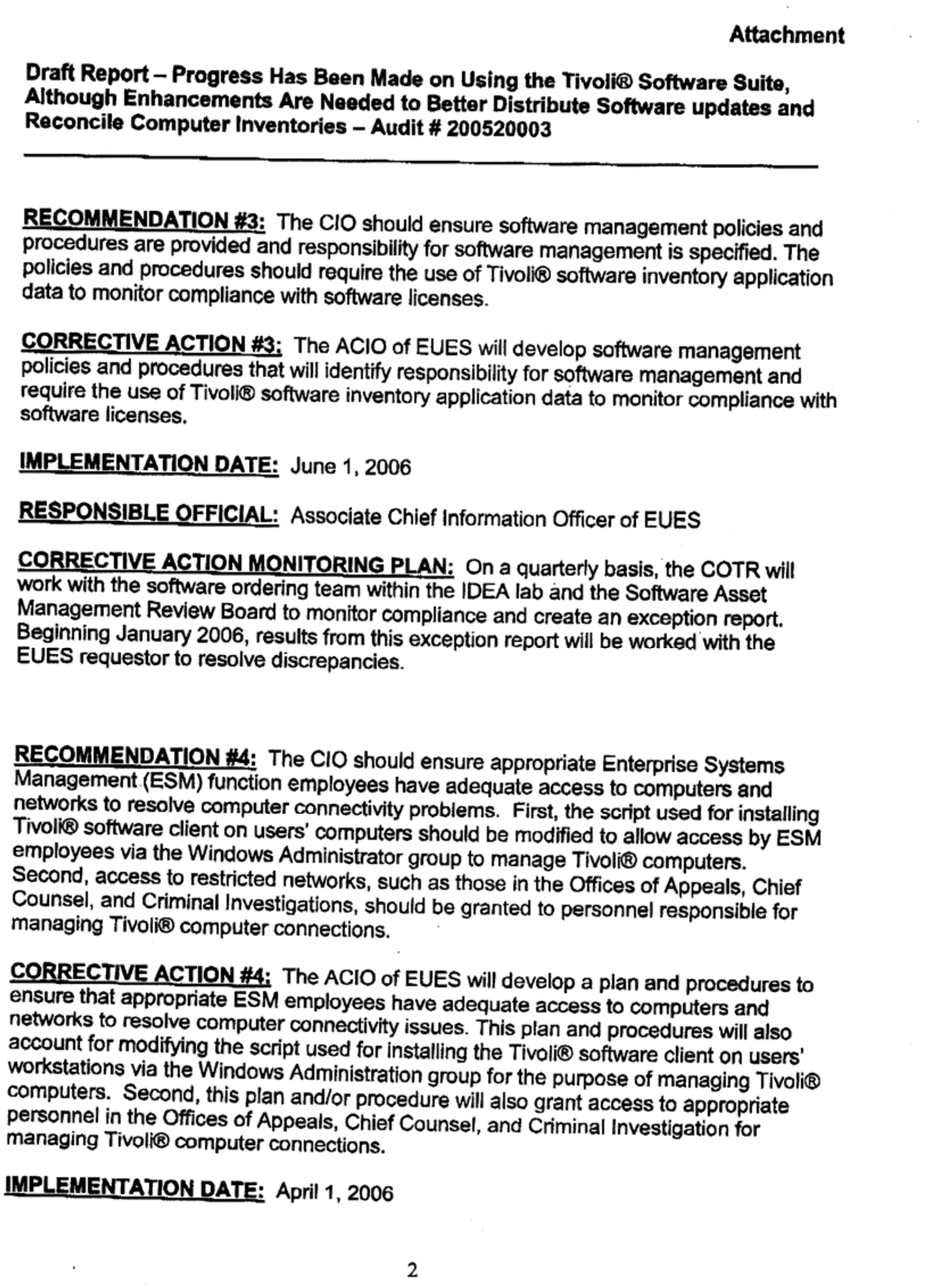
RECOMMENDATION #2: The CIO should require the Director of End User Equipment and Services to resolve mismatches between Tivoli® data and the ITAMS; and to ensure all desktops, laptops, and servers comply with the IRS' computer naming standards.

CORRECTIVE ACTION #2: The ACIO of EUES will develop appropriate procedures to resolve mismatches between Tivoli® data and the ITAMS, ensuring that all desktops, laptops, and servers comply with the IRS' computer naming standards.

IMPLEMENTATION DATE: March 1, 2006

RESPONSIBLE OFFICIAL: Associate Chief Information Officer of EUES

CORRECTIVE ACTION MONITORING PLAN: The ACIO of EUES will ensure that mismatches are resolved via the ITAMS Anomaly Report that is used to resolve other discrepancies. This report will be worked on a weekly basis.



Attachment

Draft Report – Progress Has Been Made on Using the Tivoli® Software Suite, Although Enhancements Are Needed to Better Distribute Software updates and Reconcile Computer Inventories – Audit # 200520003

RECOMMENDATION #3: The CIO should ensure software management policies and procedures are provided and responsibility for software management is specified. The policies and procedures should require the use of Tivoli® software inventory application data to monitor compliance with software licenses.

CORRECTIVE ACTION #3: The ACIO of EUES will develop software management policies and procedures that will identify responsibility for software management and require the use of Tivoli® software inventory application data to monitor compliance with software licenses.

IMPLEMENTATION DATE: June 1, 2006

RESPONSIBLE OFFICIAL: Associate Chief Information Officer of EUES

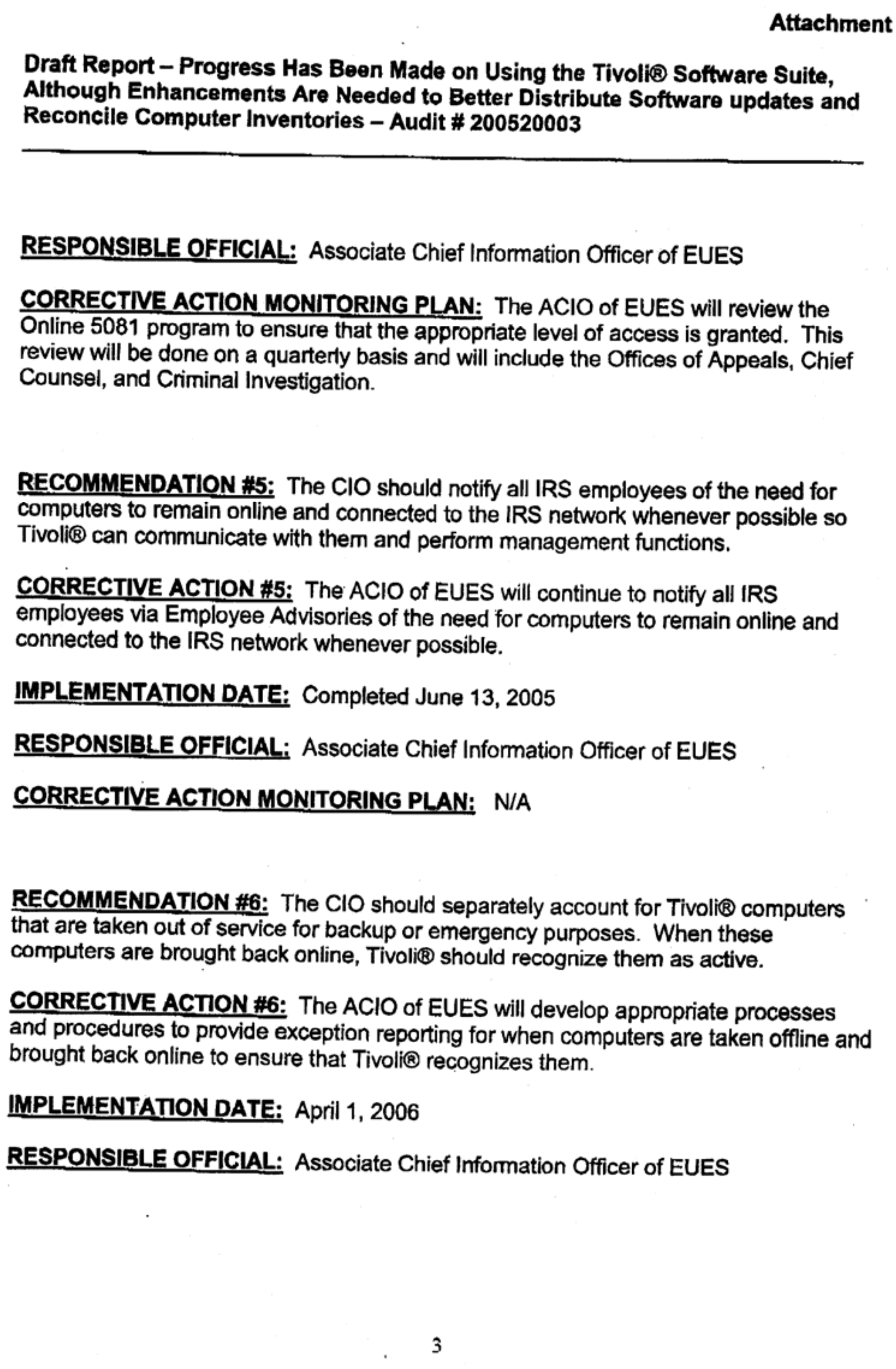
CORRECTIVE ACTION MONITORING PLAN: On a quarterly basis, the COTR will work with the software ordering team within the IDEA lab and the Software Asset Management Review Board to monitor compliance and create an exception report. Beginning January 2006, results from this exception report will be worked with the EUES requestor to resolve discrepancies.

RECOMMENDATION #4: The CIO should ensure appropriate Enterprise Systems Management (ESM) function employees have adequate access to computers and networks to resolve computer connectivity problems. First, the script used for installing Tivoli® software client on users' computers should be modified to allow access by ESM employees via the Windows Administrator group to manage Tivoli® computers. Second, access to restricted networks, such as those in the Offices of Appeals, Chief Counsel, and Criminal Investigations, should be granted to personnel responsible for managing Tivoli® computer connections.

CORRECTIVE ACTION #4: The ACIO of EUES will develop a plan and procedures to ensure that appropriate ESM employees have adequate access to computers and networks to resolve computer connectivity issues. This plan and procedures will also account for modifying the script used for installing the Tivoli® software client on users' workstations via the Windows Administration group for the purpose of managing Tivoli® computers. Second, this plan and/or procedure will also grant access to appropriate personnel in the Offices of Appeals, Chief Counsel, and Criminal Investigation for managing Tivoli® computer connections.

IMPLEMENTATION DATE: April 1, 2006

2



Attachment

Draft Report – Progress Has Been Made on Using the Tivoli® Software Suite, Although Enhancements Are Needed to Better Distribute Software updates and Reconcile Computer Inventories – Audit # 200520003

RESPONSIBLE OFFICIAL: Associate Chief Information Officer of EUES

CORRECTIVE ACTION MONITORING PLAN: The ACIO of EUES will review the Online 5081 program to ensure that the appropriate level of access is granted. This review will be done on a quarterly basis and will include the Offices of Appeals, Chief Counsel, and Criminal Investigation.

RECOMMENDATION #5: The CIO should notify all IRS employees of the need for computers to remain online and connected to the IRS network whenever possible so Tivoli® can communicate with them and perform management functions.

CORRECTIVE ACTION #5: The ACIO of EUES will continue to notify all IRS employees via Employee Advisories of the need for computers to remain online and connected to the IRS network whenever possible.

IMPLEMENTATION DATE: Completed June 13, 2005

RESPONSIBLE OFFICIAL: Associate Chief Information Officer of EUES

CORRECTIVE ACTION MONITORING PLAN: N/A

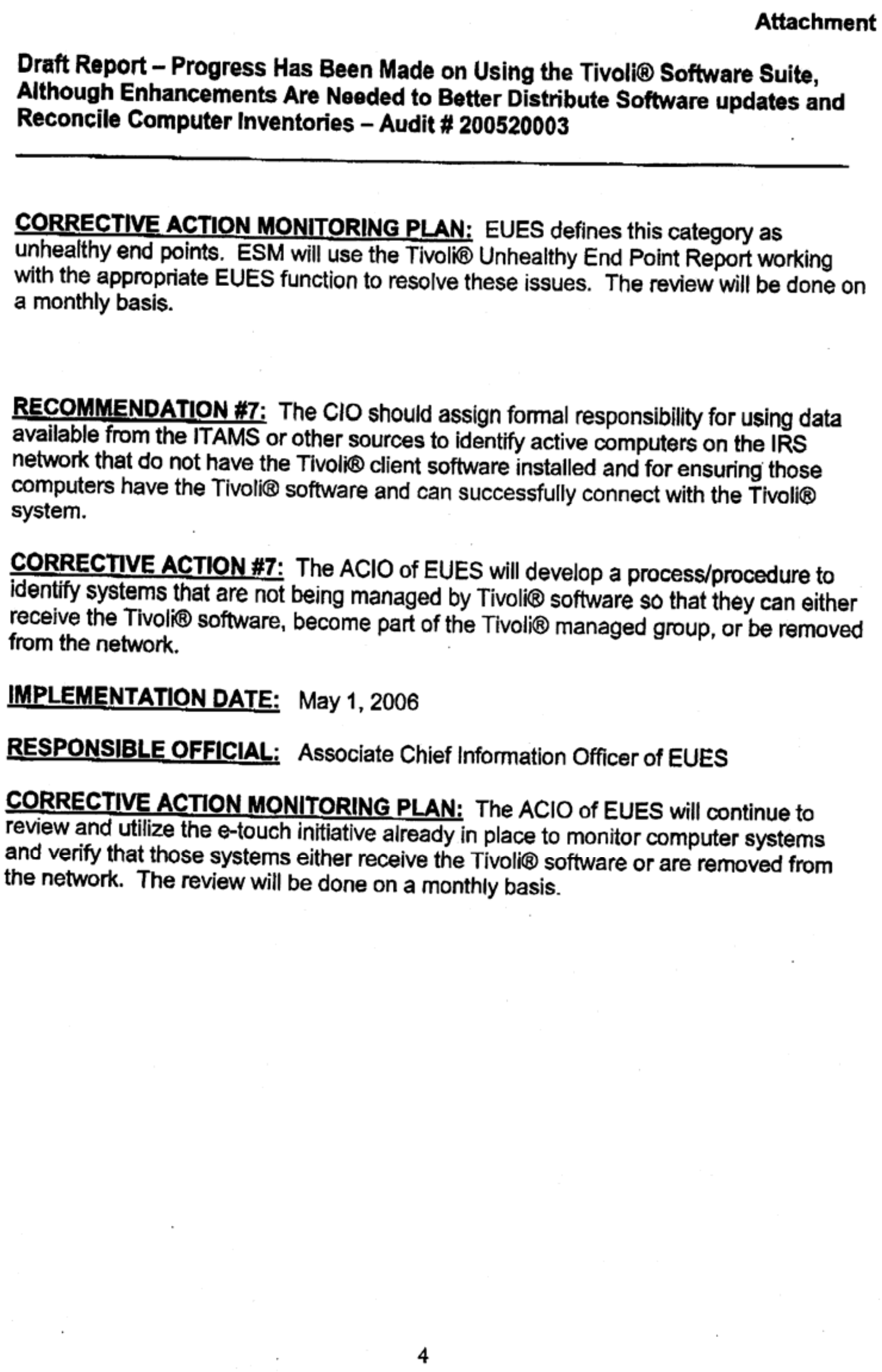
RECOMMENDATION #6: The CIO should separately account for Tivoli® computers that are taken out of service for backup or emergency purposes. When these computers are brought back online, Tivoli® should recognize them as active.

CORRECTIVE ACTION #6: The ACIO of EUES will develop appropriate processes and procedures to provide exception reporting for when computers are taken offline and brought back online to ensure that Tivoli® recognizes them.

IMPLEMENTATION DATE: April 1, 2006

RESPONSIBLE OFFICIAL: Associate Chief Information Officer of EUES

3



Attachment

Draft Report – Progress Has Been Made on Using the Tivoli® Software Suite, Although Enhancements Are Needed to Better Distribute Software updates and Reconcile Computer Inventories – Audit # 200520003

CORRECTIVE ACTION MONITORING PLAN: EUES defines this category as unhealthy end points. ESM will use the Tivoli® Unhealthy End Point Report working with the appropriate EUES function to resolve these issues. The review will be done on a monthly basis.

RECOMMENDATION #7: The CIO should assign formal responsibility for using data available from the ITAMS or other sources to identify active computers on the IRS network that do not have the Tivoli® client software installed and for ensuring those computers have the Tivoli® software and can successfully connect with the Tivoli® system.

CORRECTIVE ACTION #7: The ACIO of EUES will develop a process/procedure to identify systems that are not being managed by Tivoli® software so that they can either receive the Tivoli® software, become part of the Tivoli® managed group, or be removed from the network.

IMPLEMENTATION DATE: May 1, 2006

RESPONSIBLE OFFICIAL: Associate Chief Information Officer of EUES

CORRECTIVE ACTION MONITORING PLAN: The ACIO of EUES will continue to review and utilize the e-touch initiative already in place to monitor computer systems and verify that those systems either receive the Tivoli® software or are removed from the network. The review will be done on a monthly basis.