# TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

## *Secure Configurations Are Initially Established on Employee Computers, but Enhancements Could Ensure Security Is Strengthened After Implementation*

**February 2006**

**Reference Number: 2006-20-031**

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.

**Redaction Legend:**

10 = Trade Secret or Commercial/Financial Information

***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**

February 22, 2006

**MEMORANDUM FOR** CHIEF INFORMATION OFFICER

Michael R. Phillips

**FROM:** Michael R. Phillips
Deputy Inspector General for Audit

**SUBJECT:** Final Audit Report – Secure Configurations Are Initially Established on Employee Computers, but Enhancements Could Ensure Security Is Strengthened After Implementation (Audit # 200520008)

This report presents the results of our review of the adequacy of the Internal Revenue Service's (IRS) Common Operating Environment (COE). To ensure consistency across the IRS network and to improve security, the IRS created the COE, which is a standardized set of commercial-off-the-shelf and internally developed applications to support the needs of all IRS employees using Microsoft Windows. The COE also allows the IRS to control security configuration settings and software on its workstations by changing one master COE template and then installing it on all computer workstations across the IRS. The overall objectives of this review were to determine whether the IRS adequately developed, deployed, and maintained the COE to ensure standard security configurations on employee workstations and to evaluate the need for software applications included in the COE template.

## *Synopsis*

The IRS developed the master COE image with secure configurations incorporating Federal Government standards as well as its own standards. According to the IRS, the master COE image had been installed on 95 percent of all employee workstations as of January 2005. This effort represents a tremendous accomplishment because the IRS has over 100,000 computers. The COE generally provides updates at least twice each year and is distributed to employee workstations via automated updates.

However, once the COE was installed, security settings were not consistently maintained. In our sample of 102 computers with the COE installed, only 42 were sufficiently secure based on the

IRS' standards.[1] The remaining 60 computers complied with less than 90 percent of the computer settings prescribed by the IRS or contained at least 1 high-risk vulnerability that could be exploited to either take control of the computer or render it unusable. We also found 50 of the 102 computers contained at least 1 incorrect setting that could have allowed employees to circumvent security controls established by the master COE and inadvertently introduce security vulnerabilities into the network. Employees could also add unauthorized software to their computers. In our sample, 11 of the 102 computers contained 21 unauthorized software programs. Some of the programs were clearly not authorized for official business, such as card and board games. The weak security settings can be attributed to system administrators since they are generally the only persons authorized to change security settings on employee workstations.

Maintaining secure settings also includes correcting new vulnerabilities that are identified by software vendors or the computer industry. However, the IRS did not ensure all new vulnerabilities on employee workstations were being addressed. We found 29 of the 102 computers in our sample did not have the latest COE update version. COE updates contain the latest available security patches to address new vulnerabilities. When the automated update installation failed, employees were not aware of the failure and did not take actions to install the updates. System administrators also did not follow up to ensure the updates had been installed.

In addition, the COE image has not been installed on over 4,700 IRS workstations. Our test indicated that computers without the COE image were missing critical security patches and contained high-risk vulnerabilities, including incorrect password length and inadequate virus protection. These computers are especially susceptible to computer viruses that could render them unusable, thereby affecting productivity and disrupting operations. At the time of our review, the IRS End User Equipment and Services Division Headquarters office did not lead a formal national effort to eliminate or convert the remaining computers without the COE image. Actions taken by local offices were inconsistent.

Lastly, software licensing can be more effectively controlled on COE computers. We determined that certain COE software packages should not be included in the COE baseline version because of their costs and limited usage. For example, the full version of Adobe® Acrobat® is an advanced software package with features employees are probably either unaware of or rarely use. In practice, most IRS employees only need the Adobe® Reader, which is free software. The IRS paid approximately $2.3 million for 10 fully licensed versions of Adobe® Acrobat®. The IRS is also under agreement for annual maintenance and support for an additional $2.3 million each year. We also identified five other applications that were rarely

[1] The IRS defines a computer to meet the IRS security standards if it scores at least 90 percent compliance for the secure settings and contains no high-risk vulnerabilities when run against the IRS' own compliance-checking computer program.

used. These applications are InfoConnect, Inso Quick View Plus, Winzip, Avery Wizard, and Roxio Easy CD Creator.

One of the major disciplines of the COE configuration management process provides that periodic configuration audits be performed on the program hardware, software, and documentation to ensure products evolve properly with recorded traceability and meet program needs. Software packages that are no longer needed would have been identified had configuration reviews been completed. At the time of our review, we were not aware of any such software configuration reviews being conducted.

## Recommendations

We recommended the Chief Information Officer hold system administrators accountable for maintaining adequate security settings on computers after the COE has been deployed. The Chief Information Officer should require system administrators to run the IRS' configuration-checking program on a sample of workstations on a periodic basis or coordinate with the Chief, Mission Assurance and Security Services, to conduct the workstation security reviews and require system administrators to follow up on workstations where the COE updates were not successfully installed. All computers without the COE image should be identified and actions taken to either install the COE image, replace the computers, or manually bring the computers into compliance with prescribed security configurations. We also recommended the Chief Information Officer use available tools to identify possible unauthorized software installed on computers, consider purchasing software metering tools, and assign responsibility for monitoring software with significant license agreement costs.

## Response

The Chief Information Officer agreed with our findings and most of our recommendations. The Chief Information Officer will issue a memorandum to all workstation administrators containing the expectation for maintaining adequate security settings and has commissioned a study to ensure COE compliance capability is part of the review criteria. These two corrective actions are different than our recommendations, but we agree with the alternative actions. The Chief Information Officer has also initiated a targeted distribution of baseline COE to noncompliant workstations via a Tivoli®[2] software inventory tool, and will develop a recurring report to identify computers without the COE image and take appropriate actions to bring the computers into compliance. In addition, the Tivoli® software inventory tool will be used to identify possible unauthorized software and remove nonbusiness software. The Associate Chief Information

[2] Tivoli® is a registered trademark owned by IBM and is a software suite of applications designed to systemically deliver the most current versions of software to employees' computers and scan the network for the purpose of maintaining accurate computer inventory records.

Officer (End User Equipment and Services) currently owns a software metering tool and is in the process of gathering information and monitoring the cost and justification of the software licenses. 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.

# *Table of Contents*

# Background

The Internal Revenue Service (IRS) has over 100,000 employees to administer the nation's tax systems. One of the major challenges for such a large organization has been to provide world-class computer customer service and support to its employees in an efficient and economical manner. As the pace of technology rapidly increases and the needs of employees frequently change, the IRS looked for an enterprise-wide solution that would allow it to administer systemic changes quickly and efficiently, as well as to create a standard set of computer resources for all employees.

The IRS answered this challenge by creating the Common Operating Environment (COE), which is a standardized set of commercial-off-the-shelf and internally developed applications to support the needs of all IRS employees using Microsoft Windows. The COE allows the IRS to control configuration settings on its workstations by changing one master COE template and then installing it on all computer workstations across the IRS. This effort started in 2001 and is an ongoing process.

The master COE image has two different versions, baseline and above baseline. The baseline version contains common software programs for all employees, such as Microsoft Word and Internet Explorer. The above-baseline version includes the baseline version programs and specific software programs for specialized purposes for certain employees. Over 1,000 software programs are available for installation with the approval of appropriate IRS managers.

From a security standpoint, the COE enables the IRS to install the latest security settings on most workstations. The ability of an agency to control security settings is now required with the passage of the Federal Information Security Management Act of 2002 (FISMA),[1] which aims at strengthening the security of Federal Government data and information systems. The FISMA requires each agency to develop specific system configuration requirements that meet its own needs and to ensure compliance with these requirements. In addition, the Office of Management and Budget states effective security is an essential element of all information systems.[2] A process assuring adequate security must be integrated into an agency's management of information resources.

This review was performed in the End User Equipment and Services (EUES) Division at the Martinsburg Computing Center, Martinsburg, West Virginia; and the Area Offices in New Carrollton, Maryland; Dallas, Texas; Oakland, California; Seattle, Washington; and Manhattan, New York, during the period December 2004 through May 2005. The audit was

---

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

[2] Office of Management and Budget Circular A-130, Section 8b (3), *Securing Agency Information Systems*.

conducted in accordance with *Government Auditing Standards*. Detailed information on our audit objectives, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

# Results of Review

## The Common Operating Environment Provides Adequate Security on Employee Workstations, but Improvements Can Be Made to Ensure Security Is Maintained

The IRS developed the master COE image with secure configurations incorporating the Federal Government standards as well as its own standards. The EUES Division of the Modernization and Information Technology Services organization developed processes and procedures to ensure the master COE image is installed on most employee workstations. According to the IRS, the master COE had been installed on 95 percent of all employee workstations as of January 2005. This effort represents a tremendous accomplishment because the IRS has over 100,000 computers.

In addition, the IRS has a process in place to govern changes made to operating systems and applications of the master COE image. This process allows the IRS to maintain and keep the master image up to date. The COE generally provides updates at least twice each year and is distributed to employee workstations via automated updates from the Tivoli® applications,[3] which are operated by the Enterprise Systems Management Office of the EUES Division. While reviewing this process, we found changes or deviations to the master COE images were properly reviewed and approved.

While the master COE image provides secure settings, the settings were not maintained on computers after installation on employee workstations. In addition, workstations without the COE image[4] were not manually configured with secure settings. In both instances, high-risk vulnerabilities existed that could be exploited to either take control of the computer or render it unusable.

---

[3] Tivoli® is a registered trademark owned by IBM and is a software suite of applications designed to systemically deliver the most current versions of software to employees' computers and scan the network for the purpose of maintaining accurate computer inventory records.

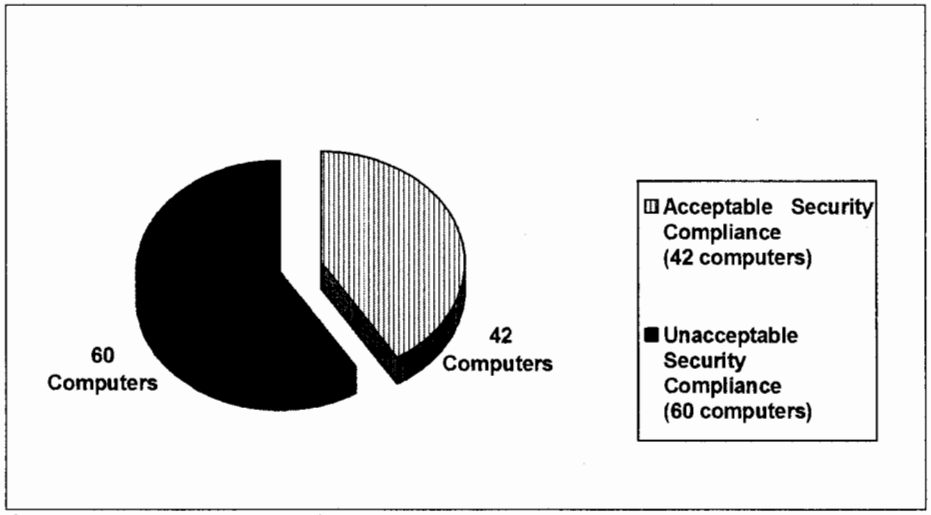
[4] The COE image cannot be installed on Windows NT computers. In addition, there may be other business reasons for not installing the COE on workstations.

## Secure settings on COE computers were not consistently maintained

The National Institute of Standards and Technology[5] recommends that, after any Windows operating system has been installed and securely configured, it must be regularly monitored and patched[6] to reduce software vulnerabilities. The IRS' policy on the Windows operating system also requires workstations be securely configured and maintained, especially when dealing with critical patches.

The IRS uses a computer application to measure the compliance of its network servers with security standards.[7] We used this application to test compliance of 102 workstations that contained the COE image. The workstations were located in five IRS offices.[8] As presented in Figure 1, we found the following compliance rates.

***Figure 1: Windows Configuration Compliance Results for 102 COE Computers Reviewed From 5 IRS Offices***




*Source: Treasury Inspector General for Tax Administration (TIGTA) results using the IRS application for measuring compliance with security standards.*

The IRS considers any computer that complies with at least 90 percent of its security standards and does not have any high-risk vulnerabilities to be acceptable from a security standpoint. Only

---

[5] The National Institute of Standards and Technology, under the Department of Commerce, is responsible for developing standards and guidelines for providing adequate information security for all Federal Government agency operations and assets.

[6] 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.

[7] This computer application was designed solely for servers. While it can be used to evaluate computer configuration compliance on workstations, the IRS does not require it to be run against its own workstations.

[8] We visited New Carrollton, Maryland; Dallas, Texas; Oakland, California; Seattle, Washington; and Manhattan, New York, to conduct this test.

42 (41 percent) of the 102 computers in our sample complied with IRS standards. The remaining 60 computers did not meet the 90 percent threshold for acceptable security compliance or contained at least 1 high-risk vulnerability. These vulnerabilities included incorrect minimum password length and lack of current virus detection definitions.

We also found significant vulnerabilities not addressed by the IRS' configuration-checking computer program. For example, 50 (49 percent) of the 102 COE computers contained at least 1 of the following incorrect security settings that could allow employees to make changes on their computers.[9]

- Of the 102 COE computers, 34 were configured to boot (i.e., start up) from a location other than the computer's hard drive. When a computer is allowed to boot from a removable media drive (e.g., compact disk), an employee as well as any hacker can bypass all security controls established on the computer's operating system, including the password access control. IRS procedures require all computers to boot only from the internal hard drive. This situation may have occurred because a system administrator incorrectly set up the computer upon deployment or did not correctly reset the boot order after working on the computer.
- Of the 102 COE computers, 37 did not have the password enabled to protect the computer's start-up process.[10] IRS procedures require all computers to have this password enabled so only authorized personnel, usually system administrators, can change the boot order and other start-up processes. When no password is enabled to protect the boot order, anyone can interrupt the computer's normal start-up sequence, access the computer's start-up settings, and change the boot order so the first drive the computer accesses is a removable media drive as opposed to the computer's hard drive. Similar to the item above, a system administrator may not have set the password upon deployment or disabled the password when working on the computer.
- Of the 102 COE computers, 35 had additional accounts established that improperly gave employees administrative rights. IRS procedures require that only authorized personnel (i.e., system administrators) have administrative rights to make changes to computer settings. Users with administrative rights could modify or disable the security settings without any authorization or approval from the Information Technology Services organization. Generally, system administrators have the ability to give a local user

[9] These three incorrect settings are different from the vulnerabilities identified by the IRS' program to evaluate compliance with Windows settings. These incorrect settings are outside of the Windows operating system environment.

[10] The computer's start-up process is represented by the Basic Input Output System (BIOS). One of the processes within the BIOS is the boot order sequence. The boot order dictates where the computer will look to begin the start-up process.

(i.e., employee) administrative rights and privileges, which may explain why this situation exists.

The weak security settings can be attributed to system administrators since they are generally the only persons authorized to change security settings on employee workstations. Because our review was a snapshot in time, we were unable to determine when and why settings on workstations had been altered or updated to produce the high-risk vulnerabilities. The IRS did not identify the vulnerabilities because there are no existing procedures to monitor employees' computer configurations. Security specialists also did not periodically check compliance of security settings on employee computers.

In addition, maintaining secure settings includes correcting new vulnerabilities that are identified by software vendors or the computer industry. The IRS has two enterprise methods to address new vulnerabilities on COE computers: biannual COE version updates and ad hoc patch installations for critical vulnerabilities. However, the IRS did not ensure all new vulnerabilities were being addressed on the COE computers in our sample. We found 29 of the 102 COE computers did not have the latest COE update version. In comparing the latest COE version update to older versions from the 29 computers, we identified 16 missing unique Microsoft Corporation security patches. None of the 16 security patches were considered critical, and 6 were classified as high risk by the IRS Computer Security Incident Response Center,[11] which is responsible for identifying and categorizing security patches applicable to the IRS. The vulnerabilities[12] associated with the six missing high-risk patches could be exploited to obtain information on the computer, perform unauthorized actions, or gain elevated privileges or total control over the computer.

COE updates were not installed because the automated updates from the Tivoli® applications were not always successful, system administrators did not follow up on unsuccessfully patched computers via the Tivoli® applications, and employees were not aware of manual procedures where they could initiate receiving the latest COE version.

One of the significant benefits of standardizing configurations on all computers is to ensure security controls have been established consistently on all computers across the IRS. The COE essentially minimizes the risk of someone compromising computers on the IRS network. However, when employees are allowed to make changes to their computers, they can negate the secure settings established by the master COE image, inadvertently introduce security vulnerabilities into the architecture, and add unauthorized software to their computers. In our

---

[11] The IRS Computer Security Incident Response Center is positioned to be proactive in preventing, detecting, and responding to computer security incidents targeting IRS enterprise information technology assets. It provides assistance and guidance in incident response and provides a centralized approach to incident handling across the IRS enterprise.

[12] These security vulnerabilities were not identified by the IRS' own configuration-checking program because the vulnerabilities were recently identified by the Microsoft Corporation after the product was released. For this reason, it is important that security patches addressing these vulnerabilities are installed to affected computers.

sample, 11 of the 102 computers contained 21 unauthorized software programs. Some of the programs were clearly not authorized for official business, such as card and board games. We were unable to determine how these programs were installed onto the computers, but 8 of the 11 computers had at least 1 of the 3 incorrect settings discussed earlier in this report, which could allow the employees to make changes to or install any program onto their computers. IRS policy states that employees are prohibited from installing or using unauthorized software on IRS equipment, which includes freeware, shareware, or public domain software. The unauthorized software could contain computer viruses, which may introduce security vulnerabilities to the workstation and possibly the IRS network.

### Computers without the COE image were not manually secured

The IRS' policy for securely configured and maintained Windows operating systems applies to all Windows computers, regardless of whether the computer has the COE image. Computers without the COE image still exist in the IRS architecture. The IRS' own Enterprise Systems Management Office reported that over 4,700 (5 percent) of approximately 100,000 IRS workstations did not contain the COE image as of Janaury 2005. Although this is a small percentage of the total computers, we are concerned because these computers contain high-risk vulnerabilities that could be exploited to either access the computers or render them inoperable. In addition, these computers could be entry points into the IRS network because of the trust relations between clients and servers and could be used to either access additional resources on the network (e.g., taxpayer data) or introduce malicious programs (e.g., worms and viruses).

We selected 16 computers without the COE image and used the IRS computer application to measure compliance with security standards. The 16 computers complied with an average of 35 percent of the IRS' security standards. In addition, all 16 computers contained high-risk vulnerabilities, ranging from incorrect minimum password length to the lack of virus detection software. Also, all 16 computers were missing critical security patches. Normally, security updates and patches are installed on computers through the Tivoli® program, which distributes updates to COE computers to ensure computers have the latest software updates and patches. For computers without the COE image, the IRS must rely on system administrators to manually install software patches. When this process breaks down, computers without the COE image could be left unprotected and vulnerable, as was the case for our sample of computers.

At the time of our review, the IRS EUES Division Headquarters office did not lead a formal national effort to eliminate or convert the remaining computers without the COE image. During our site visits, local efforts were conducted to eliminate the computers without the COE image or to install the COE images on these computers. However, system administrators were not consistent in carrying out these efforts at all sites. Some system administrators allowed employees to keep computers without the COE image for unacceptable reasons, such as personal preference, while also possessing a newer COE computer.

Ensuring 95 percent of its employees' computers have the COE image is clearly an accomplishment. However, while addressing the remaining 5 percent may seem insignificant and difficult to accomplish, the IRS is taking unnecessary risks by allowing computers with high-risk vulnerabilities to exist on its network. These computers are especially susceptible to computer viruses that could render them unusable, thereby affecting productivity and disrupting operations. For example, in May 2004 the Sasser worm[13] penetrated the IRS' internal network primarily because the appropriate patch had not been installed on vulnerable computers. As a result, the worm brought down many IRS networks, which halted operations for several days and cost about $50 million in lost tax collections and lost productivity.

## Recommendations

The Chief Information Officer should:

***Recommendation 1:*** Hold system administrators accountable for ensuring the boot process password is enabled, the boot order lists only the hard drive as the boot initiation process, and the system administrator accounts are limited to those who need them to carry out their responsibilities.

> ***Management's Response:*** The Chief Information Officer indicated there is no audit trail that identifies which workstation administrator is responsible for enabling the boot process password, so there is no way to hold them accountable. However, the Chief Information Officer will issue a memorandum to all workstation administrators that will contain the expectation that the boot process is enabled, the boot order lists only the hard drive as the boot initiation process, and the workstation administrator accounts are limited to those who need them to carry out their responsibilities.
>
> ***Office of Audit Comment:*** We concur with the alternative corrective action to our recommendation.

***Recommendation 2:*** Require system administrators to run the IRS' configuration-checking program on a sample of workstations on a periodic basis to ensure security on COE computers is maintained. Another alternative would be to coordinate with the Chief, Mission Assurance and Security Services, to conduct workstation configuration compliance checks and measure workstation security in the field.

> ***Management's Response:*** Management officials within the EUES Division and Office of Mission Assurance and Security Services agree the use of the IRS' configuration-checking program to ensure COE compliance will not adequately address

[13] The Sasser worm exploited a flaw in the Local Security Authority Subservice System on Microsoft Windows computers and transferred additional exploit code to the computer. It also probed for other computers to infect. At the very least, this worm rendered computers inoperable.

the problem, nor are there resources available to conduct periodic workstation compliance checks and remediation using the available tools and resources. However, they agree with the underlying driver of this recommendation. As such, the Chief Information Officer has commissioned a study of Patch Management and Vulnerability Assessment tools, which is currently underway. The EUES Division will ensure COE compliance capability is part of the review criteria.

***Office of Audit Comment:*** We concur with the alternative corrective action to our recommendation.

***Recommendation 3:*** Require system administrators to follow up on workstations where the COE patches cannot be successfully installed using the Tivoli® system by either physically installing the patches or contacting employees to initiate actions to have the patches installed on their computers.

***Management's Response:*** The EUES Division initiated a targeted distribution of baseline COE to noncompliant workstations via the Tivoli® system in December 2005. A recurring report will be developed to identify workstations that are below the current COE version, and the results will be posted on the Enterprise Systems Management Office web site. EUES Division Area Office and Territory managers will review the web site reports monthly and install the current COE version on those workstations found to be noncompliant.

***Recommendation 4:*** Identify all computers without the COE image and either install the COE image or replace the computers which cannot be brought up to standards. For those computers without the COE image which must be retained, the local system administrators should be accountable for maintaining secure configurations and current patches.

***Management's Response:*** The Chief Information Officer stated a recurring report will be developed to identify workstations that are below the current COE version and the results will be posted on the Enterprise Systems Management Office web site. The EUES Division Area Office and Territory managers will review the web site reports monthly and install the current COE version on those workstations found to be noncompliant. If a workstation needs to be replaced to achieve COE compliance, this action will also be initiated. In situations where COE noncompliance is required to maintain operations, the Area Office Directors will provide their Customer Relationship Management organizations with the workstation name, location, and explanation. The Area Office Customer Relationship Management staff will retain the list and follow up as appropriate. The Area Office Directors will identify a point-of-contact as the designated workstation administrator for noncompliant workstations.

***Recommendation 5:*** Use the Tivoli® software inventory application to identify possible unauthorized software installed on employee computers and require employees to justify a business need for the unauthorized software or delete it from the computer.

***Management's Response:*** The EUES Division Data Security Operations function will coordinate with the Office of Mission Assurance and Security Services to identify files likely to be associated with unauthorized software. The Tivoli® software inventory tool will be used to identify workstations on which these files reside, and the obviously nonbusiness files (e.g., games) will be immediately removed. The EUES Division will develop a repeatable process to identify potential unauthorized files and require a business justification for the continued presence of the unauthorized file on the workstation. The EUES Division Data Security Operations function will review and approve or disapprove the business justification.

## Improvements Can Be Made to Effectively Control Software Licensing on Common Operating Environment Computers

The EUES Division's Integration Development for Enterprise Automation (IDEA) lab is responsible for changing, testing, and controlling software packages added to the COE image. Software vendors usually require a license agreement that authorizes the buyer to legally use the software from the vendor. For certain COE software packages, the IRS purchased license agreements on a per-employee basis, which means the IRS must buy a software license every time the COE image is installed on a computer. The COE baseline version contains over 20 software products, 11 of which are purchased on a per-license basis. The remaining software packages are free or have enterprise license agreements, which generally means the IRS has unlimited use of that software.

Our analysis determined that certain COE software packages may not be justified for inclusion in the COE baseline version because of their costs and limited usage. The IRS could be paying millions of dollars each year for software that is not being used. We interviewed 102 IRS employees in the 5 sites we visited and asked each employee to complete a survey to determine the usage frequency of 11 COE baseline software packages. The selection of 11 COE baseline software packages, which included per-license software, was based on collaboration between our audit team and IDEA lab personnel. Figure 2 presents the results of our survey.

### Figure 2: Summary of COE Software Packages Used by Employees From Five IRS Offices

| Software Title | New Carrollton | Dallas | Seattle | Oakland | Manhattan | Total |
|---|---|---|---|---|---|---|
| Total Users Interviewed: | 20 | 20 | 20 | 21 | 21 | 102 |
| Adobe® Acrobat® | 17 | 20 | 19 | 18 | 15 | 89 (87%) |
| InfoConnect | 7 | 10 | 9 | 9 | 3 | 38 (37%) |
| Microsoft Access | 12 | 15 | 4 | 8 | 7 | 46 (45%) |
| Microsoft Excel | 20 | 20 | 16 | 16 | 14 | 86 (84%) |
| Microsoft Outlook | 20 | 20 | 19 | 17 | 20 | 96 (94%) |
| Microsoft PowerPoint | 18 | 15 | 6 | 12 | 2 | 53 (52%) |
| Microsoft Word | 20 | 20 | 15 | 19 | 17 | 91 (89%) |
| Inso Quick View Plus | 2 | 4 | 3 | 1 | 1 | 11 (11%) |
| Winzip | 7 | 15 | 5 | 6 | 11 | 44 (43%) |
| Avery Wizard | 1 | 3 | 3 | 2 | 0 | 9 (9%) |
| Roxio Easy CD Creator | 4 | 10 | 4 | 6 | 8 | 32 (31%) |

*Source: TIGTA surveys.*

We provided the names of the five COE programs with the lowest percentage of use (i.e., InfoConnect, Inso Quick View Plus, Winzip, Avery Wizard, Roxio Easy CD Creator) to the IDEA lab for consideration to remove the programs from the COE baseline version and add them into the above-baseline COE version. The IDEA lab concurred that it had already considered removing the Inso Quick View Plus program, which is a program that allows the user to read documents from several different programs, from the COE baseline version. It did not comment on the other four programs.

We analyzed cost information for the other four programs. The one COE software package with a low usage rate and an significant cost was the InfoConnect software, which is a terminal emulator to allow employees to connect to remote IRS systems. This software program costs 10 per license, or $2,667,600 for 10 licenses. Moving this program from the COE baseline version to the COE above-baseline version could save some of this cost because the IRS would pay for only the software programs requested by employees who need the program. The other software programs with low usage had low or insignificant costs.

In addition, we further analyzed the purchasing costs for some of the COE baseline software programs with high usage. We have concerns about the cost of one particular software program, Adobe® Acrobat®. The IRS paid approximately $2.3 million (10 per employee) for 10 fully licensed versions of Adobe® Acrobat®. The IRS is also under agreement for annual maintenance and support for an additional $2.3 million each year. The full version of Adobe®

Acrobat® includes features employees are either unaware of or rarely use, such as the ability to create their own Portable Document Format (PDF) file. In practice, most IRS employees only need the Adobe® Reader, which is free software available for download via the Internet, to read PDF files. We believe few employees have the necessity to create, update, or revise PDF documents for use.

One of the major disciplines of the COE configuration management process provides that periodic configuration audits be performed on the program hardware, software, and documentation to ensure products evolve properly with recorded traceability and meet program needs. Software packages that are no longer needed would have been identified had configuration reviews been completed. We were not aware of any such software configuration reviews being conducted.

In addition, the IRS did not own a software license tracking or software metering tool that could assist in identifying software use at the time of our review. Until a tool for license management and software metering is used, the IRS will be unable to establish a baseline inventory. For example, the IRS spends $28 million to $32 million annually for the Microsoft Office suite products. The IRS was unable to justify how it determined the number of licenses needed. Without the ability to track software usage and licenses, the IRS may have unused licenses available that could be redistributed or have licenses that are not needed.

## Recommendations

The Chief Information Officer should:

***Recommendation 6:*** Consider purchasing software metering tools to better evaluate software usage and related costs.

> ***Management's Response:*** The Associate Chief Information Officer (EUES) currently owns the Altiris® Software Metering Tool and is in the process of deploying the tool to workstations to begin gathering data. Data will be accumulated for 90 to 120 days to determine trends and to ensure valid sampling. Support will be transitioned to the Enterprise Systems Management Office.

***Recommendation 7:*** Assign monitoring responsibilities for significant-cost software licenses to ensure purchases are justified and needed. Unneeded or unjustified licenses should be removed and documented.

> ***Management's Response:*** The Chief Information Officer stated the process of monitoring the cost and justification of ad hoc software licenses was implemented in Fiscal Year 2005 under the authority of the Software Asset Management Review Board. Once full implementation of the Altiris® Software Metering Tool is achieved, the Enterprise Systems Management Office will develop and implement a process to gather data needed for license renewal, amendment, and/or cancellation.

**Appendix I**

# Detailed Objectives, Scope, and Methodology

The overall objective of this review was to determine whether the Internal Revenue Service (IRS) adequately developed, deployed, and maintained the Common Operating Environment (COE) to ensure standard security configurations on employee workstations. We also evaluated the need for software applications included in the COE template. To accomplish these objectives, we:

I. Determined whether the IRS met COE policies and standards.

A. Assessed the adequacy of COE policies and standards.

B. Coordinated with the IRS and conducted testing to identify COE security configuration problems on its master COE image.

C. Evaluated the COE configuration management process to determine whether the IRS had sound configuration management policies in place to govern changes made to operating systems and applications on its master COE image.

D. Assessed the current status of the COE rollout in terms of percentages of computers with and without the COE image.

E. Evaluated the IRS' effort to migrate computers without the COE image into the COE.

II. Determined whether the integrity of the COE computers was maintained after rollout.

A. Ran the IRS' own configuration-checking computer program on a judgmentally selected sample of 102 computers with the COE image and 16 computers without the COE image at 5 sites to identify high-risk vulnerabilities and the configuration-setting compliance percentage with IRS standards. Because the IRS maintained over 100,000 computers across the nation, we obtained agreement from the Director, Office of Data Security, in the End User Equipment and Services Division on our sample sizes. The five sites visited were the IRS Area Offices in New Carrollton, Maryland; Dallas, Texas; Oakland, California; Seattle, Washington; and Manhattan, New York. We used a judgmental sample because we were not projecting the audit results.

B. Obtained the most current version of the COE image and compared it against the 102 COE computers.

C. Evaluated the start-up process and boot order sequence on the 102 COE computers.

D. Assessed the adequacy of user system administrator access rights on the 102 COE computers.

E. Verified patches installed on the 102 COE computers and the 16 computers without the COE image to determine whether they were current with IRS Computer Security Incident Response Center[1] advisories.

F. Conducted an employee survey of 102 IRS employees at the 5 sites to determine the usage frequency of COE baseline-version software packages.

G. Obtained and analyzed the cost of the COE baseline-version software packages.

H. Analyzed software installed on the 102 COE computers to determine whether the software was authorized for official business.

I. Assessed the adequacy of the new COE releases and the update of the older COE computers.

[1] The IRS Computer Security Incident Response Center is positioned to be proactive in preventing, detecting, and responding to computer security incidents targeting IRS enterprise information technology assets. It provides assistance and guidance in incident response and provides a centralized approach to incident handling across the IRS enterprise.

## Appendix II

# *Major Contributors to This Report*

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)
Steve Mullins, Director
Kent Sagara, Audit Manager
Michelle Griffin, Senior Auditor
William Lessa, Senior Auditor
Jackie Nguyen, Senior Auditor
Midori Ohno, Senior Auditor
William Simmons, Senior Auditor
Stasha Smith, Senior Auditor
Esther Wilson, 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

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

RECEIVED
JAN 3 0 2006

CHIEF INFORMATION OFFICER

January 30, 2006

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: W. Todd Gram
Chief Information Officer

SUBJECT: Management Response to Draft Audit Report – Secure Configurations Are Initially Established on Employee Computers, but Enhancements Could Ensure Security Is Strengthened After Implementation – Audit # 200520008
**(I-trak # 2006-06942)**

We have read your draft audit report in reference to the Internal Revenue Service's (IRS') efforts to secure the computer environment with the Common Operating Environment (COE). We appreciate the opportunity to provide a response to the audit results and recommendations. As your report indicates, the IRS is committed to securing our workstation environment by ensuring that all IRS desktops and laptops are running the current version of the COE. Although not specifically stated in your report, we know that you are aware that our Office of Chief Counsel is not covered by this report or its recommendations.

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 low risk control deficiencies.

As you acknowledge in your report, the IRS has currently deployed and maintains the COE on over 95 percent of the workstation (desktop and laptop) environment. This accomplishment represents over five years of focused effort on the part of the End User Equipment and Services (EUES) organization. When this audit was conducted in 2004, we were operating primarily in a NT environment. At that time, IRS had over 4,700 computers that were not running COE. As of today, that number is down to 3,100, an improvement of 34 percent.

Your report indicates you found that once the COE was installed, security settings were changed by local system administrators. First, we need to clarify that these settings were changed by individuals with workstation administration privileges rather than system administrators. System administration privileges pertain to servers and your audit was focused on security settings on workstations. In the NT environment, it was difficult (if not impossible) to prevent someone with workstation administrative privileges from changing security settings.

However, as we move into Active Directory (AD), we are already implementing processes that will correct this issue. Also in the NT environment, lack of granularity in the NT security settings necessitated the extension of workstation administrative privileges to non-IT personnel. EUES is currently removing workstation administration privileges from non-IT personnel and the implementation of AD will allow us to further restrict or eliminate the need for non-IT personnel to have these privileges. In addition, while the COE is a major tool for ensuring the security of our workstations, it is not the only way we ensure systems are running current Microsoft Operating System patches. We have a separate process to deploy and install current Microsoft Operating System patches outside of the COE process. Therefore, if a workstation is not running a current version of the COE it is still possible for it to be completely protected from security vulnerabilities found in the Microsoft Operating System.

We agree that we need to improve our efforts in the area of software licensing. MITS has procured a software metering tool and we are nearing the completion of its deployment. EUES will be using data gathered by that tool to help assess our true licensing needs. We have also undertaken efforts to examine all existing enterprise level software agreements, beginning with our Microsoft contract, to ensure that we are getting maximum return on our investment. We will review all user software included in the COE baseline image and ensure it is appropriate for all IRS users.

The EUES organization continues to improve the control and security of the IRS workstation environment. The number of non-compliant systems, while significant in number, represents a small percentage of the total IRS workstation environment. EUES is committed to continually improving our control and security; however the final few percentage points will be the most difficult and costly to address.

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

Attachment

**Attachment**

**Draft Report - Secure Configurations Are Initially Established on Employee Computers, but Enhancements Could Ensure Security Is Strengthened After Implementation – Audit # 200520008**

---

**RECOMMENDATION #1:** The CIO should hold systems administrators accountable for ensuring the boot process password is enabled, the boot order lists only the hard drive as the boot initiation process, and the system administrator accounts are limited to those who need them to carry out their responsibilities.

**CORRECTIVE ACTION #1:** There is no trail that identifies which workstation administrator is responsible for enabling the boot process password, so there is no way to hold them accountable. However, the CIO will issue a memorandum to all workstation administrators, through the appropriate management channels, containing the expectation that the boot process is enabled, that the boot order lists only the hard drive as the boot initiation process, and that the workstation administrator accounts are limited to those who need them to carry out their responsibilities.

**IMPLEMENTATION DATE:** March 1, 2006

**RESPONSIBLE OFFICIAL:** ACIO, EUES

**CORRECTIVE ACTION MONITORING PLAN:** The ACIO, EUES will ensure that the memorandum is prepared and distributed to all managers of systems administrators.

**RECOMMENDATION #2:** The CIO should require system administrators to run the IRS configuration checking program on a sample of workstations on a periodic basis to ensure security on COE computers is maintained. Another alternative would be to coordinate with the Chief, Mission Assurance and Security Services to conduct workstation configuration compliance checks and measure workstation security in the field.

**CORRECTIVE ACTION #2:** EUES and Mission Assurance (MA) are in agreement that the use of the automated tool, LEM Checker to ensure COE compliance will not adequately address the problem, nor are there resources available to conduct periodic workstation compliance checks and remediation using available tools and resources. However, EUES and MA both agree with the underlying driver of this recommendation. The CIO has commissioned a study of Patch Management / Vulnerability Assessment tools, which is currently underway and EUES will ensure COE compliance capability is part of the review criteria. A recommendation is targeted for April 2006, with a 12-18 month procurement and deployment schedule thereafter.

**IMPLEMENTATION DATE:** November 1, 2007

**Attachment**

**Draft Report - Secure Configurations Are Initially Established on Employee Computers, but Enhancements Could Ensure Security Is Strengthened After Implementation – Audit # 200520008**

---

**RESPONSIBLE OFFICIAL**: ACIO, EUES

**CORRECTIVE ACTION MONITORING PLAN**: The Program Manager, EAP will ensure the configuration checking capability is added to product evaluation.

**RECOMMENDATION #3**: The CIO should require system administrators to follow-up on workstations where the COE patches cannot be successfully installed using the Tivoli system by either physically installing the patches or contacting employees to initiate actions to have the patches installed on their computers.

**CORRECTIVE ACTION #3**: EUES initiated a targeted distribution of baseline COE to non-compliant workstations via Tivoli in December 2005. A recurring report will be developed to identify workstations that are below the current COE version and the results will be posted on the Enterprise Systems Management website. The Areas/Territories will review the website reports monthly and install the current COE version on those workstations found to be non-compliant.

**IMPLEMENTATION DATE**: June 1, 2006

**RESPONSIBLE OFFICIAL**: ACIO, EUES

**CORRECTIVE ACTION MONITORING PLAN**: Area Directors will report the results of their COE repairs to the Program Manager, PCAM on a quarterly basis.

**RECOMMENDATION #4**: The CIO should identify all computers without the COE image and either install the COE image or replace the computers which cannot be brought up to standards. For those computers without the COE image which must be retained, the local system administrators should be accountable for maintaining secure configurations and current patches.

**CORRECTIVE ACTION #4**: A recurring report will be developed to identify workstations that are below the current COE version and the results will be posted on the Enterprise Systems Management website. The Areas/Territories will review the website reports monthly and install the current COE version on those workstations found to be non-compliant. If there is a need to replace workstations to achieve COE compliance, this action will also be initiated. In situations where COE non-compliance is required to maintain operations, the Area Directors will provide their CRM organizations with the workstation name, location, and explanation. The Area CRM staff will retain the

**Attachment**

**Draft Report - Secure Configurations Are Initially Established on Employee Computers, but Enhancements Could Ensure Security Is Strengthened After Implementation – Audit # 200520008**

---

list and follow-up, as appropriate. The Area Directors will identify a point-of-contact as the designated workstation administrator for non-compliant workstations.

**CORRECTIVE ACTION MONITORING PLAN:** For those workstations which cannot be re-imaged and have a valid business justification, the CRM staff will be responsible for maintaining a record and will validate the business need quarterly. Each point-of-contact will certify via email quarterly to the CRM staff that all non-COE workstations under their span of control have a secure configuration and that all current patches are installed.

**IMPLEMENTATION DATE:** October 1, 2006

**RESPONSIBLE OFFICIAL:** ACIO, EUES

**RECOMMENDATION #5:** The CIO should use the Tivoli software inventory application to identify possible unauthorized software installed on employee computers. The CIO should require employees to justify a business need for the unauthorized software or delete it from the computer.

**CORRECTIVE ACTION #5:** EUES Data Security Operations (DSO) will coordinate with Mission Assurance & Security Services to identify .exe files likely to be associated with unauthorized software. The Tivoli software inventory tool will be used to identify workstations on which these .exe files reside and those .exe files that are obviously games will be immediately removed using Tivoli tools. EUES will develop a repeatable process to identify potentially unauthorized .exe files (non-games) and require a business justification for the continued presence of the .exe file on the workstation. The EUES, DSO will review and approve/disapprove the business justification.

**IMPLEMENTATION DATE:** October 1, 2006

**RESPONSIBLE OFFICIAL:** ACIO EUES

**CORRECTIVE ACTION MONITORING PLAN:** Enterprise Systems Management will monitor implementation and provide quarterly status reports to PCAM until a repeatable process is established. After that, DSO will provide an annual status report to PCAM.

**Attachment**

**Draft Report - Secure Configurations Are Initially Established on Employee Computers, but Enhancements Could Ensure Security Is Strengthened After Implementation – Audit # 200520008**

---

**RECOMMENDATION #6:** The CIO should consider purchasing software metering tools to better evaluate software usage and related costs

**CORRECTIVE ACTION #6:** The ACIO, EUES currently owns the Altiris Software Metering Tool and is in the process of deploying the workstation clients to begin gathering data. Data will be accumulated for 90-120 days to determine trends and to ensure valid sampling. Support will be transitioned to Enterprise Systems Management.

**IMPLEMENTATION DATE:** August 1, 2006

**RESPONSIBLE OFFICIAL:** ACIO, EUES

**CORRECTIVE ACTION MONITORING PLAN:** Status reports will be provided to ACIO, EUES on a monthly basis to provide results on deployment and data gathered.

**RECOMMENDATION #7:** The CIO will assign monitoring responsibilities for significant cost software licenses to ensure purchases are justified and needed. Unneeded or unjustified licenses should be removed and documented.

**CORRECTIVE ACTION #7:** The process of monitoring the cost and justification of ad hoc software licenses was implemented in FY05 under the authority of the Software Asset Management Review Board (SAMRB). Once full implementation of Altiris is delivered from the project to operations, Enterprise Systems Management will develop and implement a process to gather data needed for license renewal, amendment, and/or cancellation.

**IMPLEMENTATION DATE:** January 2, 2007

**RESPONSIBLE OFFICIAL:** ACIO, EUES

**CORRECTIVE ACTION MONITORING PLAN:** The statistical information gathered as a result of the monitoring will be provided to the ACIO, EUES.