Audit Report

OIG-11-112

INFORMATION TECHNOLOGY: BEP's Network and Systems Security Was Found to Be Insufficient

September 30, 2011

Office of Inspector General

DEPARTMENT OF THE TREASURY

Contents

Audit Report

Appendices

Abbreviations

BEP	Bureau of Engraving and Printing
BIOS	Basic Input Output System
CIO	Chief Information Officer
HTTPS	Hypertext Transfer Protocol Secure
IT	Information Technology
JAMES	Joint Audit Management Enterprise System
OCIO	Office of the Chief Information Officer
OIG	Treasury Office of Inspector General
OPTR	Office of Privacy, Transparency, and Records
OMB	Office of Management and Budget
USB	Universal Serial Bus

OIG

Audit Report

The Department of the Treasury
Office of Inspector General

September 30, 2011

Larry R. Felix
Director
Bureau of Engraving and Printing

The objective of this audit was to determine whether sufficient protections were in place to prevent and detect intrusions into the Bureau of Engraving and Printing's (BEP) network and systems.

To accomplish our objective, we performed an internal vulnerability assessment and penetration test of BEP's network and systems. We also tested BEP's internet-facing websites external to BEP's network using only information available to the general public. Additionally, we performed a social engineering test to determine whether BEP users were aware of, and carrying out their responsibilities, in protecting the bureau's information technology (IT) resources.

We performed our fieldwork at BEP headquarters location in Washington, DC, from May 2010 through April 2011. The audit was performed in accordance with generally accepted government auditing standards. Our objectives, scope, and methodology are described in appendix 1.

Results in Brief

We determined that BEP did not establish sufficient protection for its network and systems and should enhance its security controls to protect against threats posed by malicious insiders. Specifically, during our social engineering exercise, we successfully persuaded 23 BEP users to give us access to their computers (100 percent of those attempted) using their accounts. While impersonating BEP contractors with unescorted access to the facility, every user whom we approached gave us full access to their computer without challenge. In fact, in one instance, a BEP employee observed us standing at the door to a restricted area. Rather than question our presence, he opened the door and let us in, giving us unescorted access to the entire administrative area.

Our work also identified significant deficiencies in BEP's network and systems related to its patch management processes and system configurations. Specifically, we found critical vulnerabilities because of a number of missing security patches, some more than 1 year old. For example, we were able to gain system-level access to a BEP desktop missing an 8 year old patch, and user-level access to a BEP server missing a 3 year old patch. By taking advantage of these vulnerabilities, we were able to gain full access to the desktop, where we were able to create, edit, delete, and move files. We were also able to access files and databases on the server.

Finally, we noted that BEP did not fully comply with the Office of Management and Budget (OMB) Memorandum M-10-22, "Guidance for Online Use of Web Measurement and Customization Technologies" (June 25, 2010). This memorandum emphasizes the need to safeguard the privacy of the American public while increasing the Federal Government's ability to serve the public by improving and modernizing its activities online. To that end, the guidance applies to any Federal agency use of web measurement and customization technologies by providing clear, firm, and unambiguous protection against any uses that would compromise or invade personal privacy. This guidance is not limited to any specific technology or application (such as persistent cookies),[1] and includes Federal agency use of third-party web measurement and customization technologies.

Considering the deficiencies we identified during the course of this audit and subsequent discussions regarding them with the BEP Chief Information Officer (CIO) and his staff, we were concerned over the state of BEP's network and systems security and what we found to be a lack of effective oversight exercised by its CIO.

[1] The term "cookie" covers a wide array of techniques used to track information about web site usage. This report uses the term as shorthand for "persistent cookie," a web technology that can track the activity of users over time and across different web sites. (From OMB "Cookies Letter, 07-28-00," http://www.whitehouse.gov/omb/inforeg_cookies_letter72800). OMB M-10-22 identifies persistent cookies as a specific technology used in web measurement and customization.

We are making a number of recommendations to the Director of BEP to address the weaknesses identified during the course of this audit. Among those recommendations are the need to reinforce and enhance security awareness training, emphasizing the malicious insider threat, conduct periodic social engineering tests to assess the effectiveness of user security awareness training, improve BEP's patch management process to ensure that all critical patches are applied on a timely basis, and ensure the antivirus central server and the intrusion detection system records and maintains all information security alerts.

In a written response to a draft copy of this report, BEP management provided us with its planned corrective actions, and discussed those corrective actions it already has underway. BEP's response meets the intent of our recommendations. BEP's written response is included in appendix 2.

Background

The Federal Information Security Management Act, Title III of the E-Government Act of 2002, requires each federal agency's information security program to provide information security for the information and information systems that support the operations and assets of the agency. The program should include periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification or destruction of information and information systems that support the operations and assets of the agency. Specifically, agencies are required to perform periodic testing and evaluation of management, operational, and technical controls of information systems depending on risks; and institute a process for planning, implementing, evaluating and documenting remedial action to address any deficiencies or exploits. An independent network and system security assessment, like this one, is performed to validate the controls that have been put in place are functioning properly.

BEP's mission is to design and manufacture high quality security documents that deter counterfeiting and meet customer requirements for quality, quantity, and performance. BEP's primary function is to print billions of dollars, referred to as Federal Reserve Notes, each year for delivery to the Federal Reserve System. As the government’s printer, the BEP’s customers and stakeholders expect and demand the highest degree of security. An unauthorized attack or system intrusion on BEP’s network and systems could be detrimental to that mission by putting at risk the government’s ability to print paper money and other security documents.

Findings and Recommendations

Finding 1 Security Awareness Training Program Did Not Harden Users Against Social Engineering Attacks

We determined that BEP’s security awareness training program did not harden users against social engineering attacks. As a consequence, users allowed unknown individuals, our auditors posing as BEP contractors, complete access to their computers. During our social engineering test, we successfully persuaded all 23 BEP users we approached (100 percent) to give us full access to their computers without challenging our credentials. Specifically, we approached the users and asked them if we could “check the antivirus software” installed on their computers without identifying ourselves. We intentionally turned our BEP-issued contractor badges inward so that the users could not see our names and pictures on the badges. Even though we were unknown to the users we approached, none of them challenged us or asked to see our badges or any paperwork. In short, these users allowed individuals, whose only visible credential was the back side of a contractor badge, complete access to their computers.

At each system, we either asked the user to stay logged in or to log back in for us. Some of these users stayed and watched us use their computers (e.g., extracting files, running executables, and using the command prompt), while others left us alone. In every case, we were given complete access to the computer without the user visibly displaying any degree of skepticism or even asking our names. Once on the computer, we took full control with the user’s access level. We then used applications stored on our Universal Serial Bus (USB) thumb drive and Compact Disc we brought with us to extract data from their computers and view their files. As a result, we were able to, among other things, find and extract Personally Identifiable Information from some of the computers.

Examples of the types of Personally Identifiable Information we were able to access included BEP employee names, social security numbers, places of birth, time in government, entry on duty dates, and mid- and end-of-year performance appraisals.

On one occasion, a BEP employee held the door open, allowing us to enter a restricted administrative area unescorted. At the time, our badges were still facing inward, and the employee did not challenge our motives for entry. Once inside the secured area, we were able to gain access to additional computers.

On the 2nd day of our social engineering test, the BEP Chief of Office of Critical Infrastructure and IT Security told us that five BEP users from the previous day's social engineering test had verbally reported our activities. However, BEP was not able to provide us with any help desk tickets documenting those reports.

The other 18 users did not report our activities to anyone. Therefore, at best, five targeted users were suspicious enough of our activities to call security after we left, but not suspicious enough to ask our names or to see our credentials before allowing us access to their computers. The other 18 users displayed no concern or presumably deemed our presence as nothing more than a minor disruption.

All BEP users must sign BEP IT Rules of Acceptable Use Form 8394 (Rev. 1-08). These rules require, among other things, that users not let anyone else use their account or associated account privileges. Users are also supposed to notify the system administrator, the help desk, or the IT Security Division of any unusual occurrences during logging in or signing off or during use of their computer. In short, the rules clearly state that users are responsible for protecting any information used or stored by their account and those users must report any incidents of possible misuse, suspected viruses or IT security incidents or weaknesses in IT security to the help desk.

Based on this test, even though BEP had an established annual user security awareness training program, we found an alarmingly high failure rate of BEP's security awareness practices.

When we spoke subsequently with several users who had given us access to their computers, they told us that they did not remember the same set of circumstances that we presented to them. For example, one user said that he thought his computer was logged-off when he left us at his desk, and another user said that he assumed we were contractors from BEP's help desk.

We believe BEP users' susceptibility to these types of attacks may be attributed to, at least in part, the lack of regular social engineering training. Part of this training would include unannounced social engineering tests to reinforce user awareness and provide an understanding of how users can defend themselves and BEP against social engineering attacks. BEP could also use these opportunities to communicate the possible consequences of a breach to include compromising the confidentiality, integrity, and availability of BEP information.

Recommendations

We recommend that the Director of BEP do the following:

1. Reinforce and enhance through BEP's regular user awareness training the following social engineering countermeasures:
   - Users should be instructed/reminded to request the identification of unfamiliar individuals who are requesting access to their BEP computers.
   - Users should be instructed/reminded to log-off or lock their computers any time they leave their computers unattended.
   - Users should be instructed/reminded to not allow anyone else to use their BEP credentials or accounts, including those from the BEP help desk.
   - Users should be instructed/reminded to not allow anyone into secure areas without valid credentials.
   - Users should be instructed/reminded to inform BEP help desk if they notice unauthorized individuals accessing BEP computers or secure areas.

Management Response

BEP management stated that its employees are required to take the required training program established and maintained by Treasury on the Treasury Learning Management System. BEP will request that the Treasury office that manages the training program include additional instructions related to the risk posed by malicious insiders. Additionally, BEP will prepare an "All Employee E-mail" and an article in the monthly Communicator to reinforce the items in the recommendation.

OIG Comment

Management's planned corrective actions are responsive to our recommendation. BEP management will need to establish definitive dates for when they expect these corrective actions to be implemented.

2. Conduct periodic social engineering tests to assess the effectiveness of user security awareness training.

Management Response

BEP management stated that it will augment its current testing with additional scenarios associated with malicious insider threats similar to those utilized during this test. The first roll out of these new tests will occur prior to the end of calendar year 2011.

OIG Comment

Management's planned corrective action is responsive to our recommendation

Finding 2 BEP's Patch Management Process Was Not Effective in Protecting Its Network and Systems

We determined that BEP's patch management[2] process was not effective because a substantial number of critical[3] patches were missing from bureau desktops and servers. As a result, BEP's

[2] Patch management is a security practice designed to prevent the exploitation of IT vulnerabilities that exist within an organization. The expected result is to reduce the time and money spent dealing with vulnerabilities and exploitation of those vulnerabilities.

[3] A critical vulnerability is a remote exploit, granting root or administrator access, or having an active worm or virus spread in the public realm.

network and systems were not fully safeguarded, leaving them vulnerable to attacks from malicious insiders. We also found that BEP management did not document its rationale for not applying critical patches.

We scanned 1,136 desktops at BEP headquarters in Washington, DC, and found that BEP's desktops were missing a total of 220 critical patches. Of those 220 missing critical patches, 60 percent were more than 1 year old. Similarly, we scanned 95 servers at BEP, and found those servers were missing a total of 152 critical patches. Of those 152 missing critical patches, 50 percent were more than 1 year old. In all, over half of the missing critical patches we identified were more than 1 year old without any documented explanation as to why BEP did not install the patches.

Among the missing critical patches that we identified were one from a desktop, missing since 2002, and one from a server, missing since 2007. Using that information, we were able to successfully exploit both the desktop and server.

With regard to the desktop exploitation, we were able to gain remote system-level access on that computer. This access allowed us to create, edit, delete, and move files. It enabled us to remotely retrieve files, take screenshots, and run our programs on the target desktop. We were also able to extract the local Security Accounts Manager[4] file and decrypt the password of a local account with administrative privileges for that computer.

During this process, we viewed real-time user activity. For example, we saw a BEP user viewing a scanned copy of a $10 note on his desktop. Our remote view of the compromised desktop also allowed us to see that the user appropriately received an antivirus notification, while our attack was taking place. To our surprise, however, we also saw that user disregard the antivirus notification by moving it to the bottom of the screen, and continue to work. Appendix 3 contains two remote screenshots we took of the exploitation just described; the screenshots capture the real-time antivirus notification that was received by the user and the

[4] Security Accounts Manager is a registry file in Windows NT, Windows 2000, and later versions of Windows. It stores users' passwords in a hashed format (in LM hash and NTLM hash). Obtaining this information enables someone to decrypt passwords.

user moving that notification to bottom of the screen so that he could continue to work. It should be noted that portions of the screenshots included in appendix 3 have been redacted.

Following up on the antivirus notification, BEP management told us that the antivirus central server did not log this incident. BEP followed-up with the vendor of the antivirus software to determine why the antivirus central server failed to log the incident. At the time of this report, the software logging failure remained unresolved.

With regard to our server exploitation, we were able to gain user-level access, allowing us to create, edit, delete, and move files, as well as access a database. Similar to the desktop exploitation, BEP's intrusion detection system failed to log our activities on the server.

In interviews with BEP management, we were told that the IT Security Division (IT Security) is responsible for identifying vulnerabilities in BEP's network and systems and reporting them to the IT Technical Support Division (IT Operations) for remediation via a ticketing system. However, we found that not all of these vulnerabilities were being remediated. According to the IT Operations Chief, some tickets were being closed without full remediation. IT Security told us they ran regular vulnerability scans and generated a help desk ticket so that IT Operations could remediate the vulnerabilities discovered by the scans. IT Operations would then apply most of the patches and close the ticket because some of the patches were deemed not applicable or would present a risk to some IT resources. However, IT Operations did not document the rationale/business reasons why these patches were not applied. Also, IT Security could not tell us if the same vulnerabilities were discovered in consecutive scans because they did not analyze of the vulnerabilities to determine if the same vulnerabilities were repeatedly being reported.

We were so concerned about what we had found that we provided BEP's CIO staff with the reports generated by our automated assessment tools in July 2010, so that timely corrective actions could be taken. The reports provided details on specific vulnerabilities detected and exploited, and the suggested actions needed to address them.

During the Notifications of Findings and Recommendations meeting held in January 2011, we were surprised to learn that BEP had not reviewed the reports because they found the tool-generated reports too copious. Therefore, no corrective action or mitigation was taken with respect to the vulnerabilities that we had identified 6 months earlier.

According to BEP IT Security Policy and Procedures Manual, No. 10-08.35 (August 1, 2005), the manager of IT Operations is responsible for ensuring that systems and applications are maintained with the proper updates and security patches, and for providing status on the state of the current IT infrastructure, to include implementing, documenting, and monitoring patches, workarounds and updates. Treasury CIO memorandum M-06-01, "Improving the Department's Security Plan of Action and Milestone Process" (March 24, 2006)[5] requires that security weaknesses be entered into the Plan of Action and Milestones to provide an auditable trail of the weakness remediation. Treasury Directive Publication 85-01, "Treasury Information Technology Security Program" (June 9, 2009), control S-PM.2 requires that bureaus ensure security patches are tested and installed on a timeline in accordance with the criticality of the patches. Additionally, the National Institute of Standards and Technology Special Publication 800-61, "Computer Security Incident Handling Guide" (March 2008), states that organizations should establish logging standards and procedures to ensure that adequate information is collected by logs and security software.

BEP management was unable to provide us any reason for not applying the critical patches that were over 1 year old. Furthermore, IT Operations did not document the business reasons/rationale for not applying patches. The BEP IT Operations Chief acknowledged that there was no documentation for patches that were not applied, and that the unapplied patches were not entered into the Plan of Action and Milestones process as required by the Treasury CIO Memorandum M-06-01 for security

[5] Agency CIOs, working with other appropriate agency officials, are responsible for developing a POA&M for each program and system for which a weakness was identified. The purpose of a POA&M is to help agencies identify, assess, prioritize, and monitor progress of corrective efforts for security weaknesses in programs and systems.

weaknesses. We believe this deficiency is due, at least in part, to the absence of an adequate patch tracking system in IT Security and lack of oversight by the managers of IT Operations, IT Security, and the CIO.

If BEP does not apply patches in a timely manner, the vulnerabilities resulting from these missing patches could put BEP's systems at risk for exploitation by internal and external hackers. As evidence, we compromised two systems using exploits known to the manufacturer who recommended patches 3 and 8 years, respectively, prior to our tests.

In addition, the lack of comprehensive incident reporting further hampers BEP's efforts to detect attackers and deter them from gaining access to BEP's systems. Our test exposed a failure of both the user and the antivirus central server to identify and alert management of the security compromise. Had our attacks been malicious, BEP would not even have been aware that we compromised the targeted systems or any of the information residing on those systems.

Recommendations

We recommend that the Director of BEP do the following:

3. Improve the patch management process to ensure that all critical vulnerabilities are patched, mitigated, or justified as to why the risk of not patching was accepted (e.g., business reasons) in a timely manner. Additionally, vulnerabilities are to be documented in the Plans of Action and Milestones as specified in TCIO M-06-01.

Management Response

BEP management stated that it will continue to improve the patch management process by proactively addressing flaws exposed in deployed hardware and software products and remains committed to following best practices regarding patch management and maintaining a defense-in-depth architecture to manage risks throughout the enterprise.

OIG Comment

Management's planned corrective action meets the intent of our recommendation. However, we would like to emphasize that the critical vulnerabilities that we identified allowed us unauthorized access to sensitive information. Furthermore, BEP will need to review the missing patches that allowed for the critical vulnerabilities that we identified and determine whether to mitigate or accept the vulnerabilities as risks. In addition, unmitigated vulnerabilities are to be documented in the Plans of Action and Milestones as specified in TCIO M-06-01. BEP management will need to establish definitive dates that these planned actions are expected to be completed in JAMES.

4. Ensure the intrusion detection system and the antivirus central server are corrected to properly log all information alerts generated by desktops and servers.

Management Response

BEP management stated that it contacted the relevant vendors to review and verify the system configurations and confirmed the systems are functioning correctly to properly log all information alerts.

OIG Comment

Management's corrective action meets the intent of our recommendation.

Finding 3 Some BEP Systems Were Configured With Ineffective Security Settings

We found that some of BEP systems were configured with ineffective security settings, resulting in critical vulnerabilities. As we demonstrated, some of these vulnerabilities put BEP systems at risk of exploitation by malicious insiders. With that said, many of these vulnerabilities could be eliminated through modification of security settings.

Below are the categories of vulnerabilities we found in some BEP systems during our social engineering and penetration tests that resulted from ineffective security settings:

- Lack of full disk encryption. The hard drives of some desktops were not encrypted, which allowed us to easily gain access to BEP data.

- Basic input output system (BIOS)[6] open access. Some BEP systems were found with BIOS settings that allowed booting from alternate media devices without password prompting. This enabled us to bypass the security controls on the desktops.

- Unauthorized USB devices allowed. Some of the systems we tested allowed us to use unauthorized USB devices to access data on the systems.

- Open Windows registry access[7]. One system we tested allowed user access to the Windows registry. The availability of the registry allowed us to gather more complete and accurate information about the system we were attacking.

- Open ports. Some printers and computers were configured with open network service and telnet ports when not required by any business need.

- Weak X.509 certificate encryption. We found some systems were using weak algorithms to encrypt their certificates, which are used to authenticate computers over the BEP local area

[6] BIOS is the first code run by a computer when powered on. The BIOS primarily determines which operating system should be loaded.

[7] Microsoft Windows Registry is a hierarchical database that stores configuration settings and options on Microsoft Windows operating systems.

network.

- Weak Hypertext Transfer Protocol encryption. We found that some BEP systems were not using Hypertext Transfer Protocol Secure (HTTPS). It is an acknowledged best practice to implement HTTPS wherever possible to prevent the accidental transmission of sensitive information.

- Anonymous user login[8]. We found that some systems were allowing access to Oracle and network services with anonymous or null accounts, which could grant an attacker access to network services without requiring authentic user credentials.

We exploited the first four of these vulnerabilities to extract personal and official information from BEP users' computers in the presence of those users during our social engineering test.

According to the National Institute of Standards and Technology Special Publication 800-53, "Recommended Security Controls for Federal Information Systems and Organizations" (May 2010), organization should configure the information to provide only essential capabilities. Additionally, the SANS Institute InfoSec Reading Room paper entitled, Why Bother About BIOS Security, recommends that passwords be used on every computer in order to protect the BIOS configuration utility.

According to BEP's Chief of Office of Critical Infrastructure and IT Security, the risks associated with some of the vulnerabilities were accepted due to business needs. However, there was no documentation supporting those determinations. For the other vulnerabilities that were identified, no explanation was provided. We believe this is because either BEP was unaware the

[8] An access control quality, which can be a weakness, where a lot of secure servers allow users to access general-purpose or public services and resources without owning a user-specific account that is pre-established, something like a user name or secret password, lowering internet security and network security because there is no secure authentication.

vulnerabilities existed or unable to effectively manage the variety of hardware and software configurations in their environment.

These categories of vulnerabilities could be exploited by malicious insiders in various ways, leaving BEP's systems at risk of data exposure, modification or deletion. Moreover, taking advantage of these vulnerabilities, we were able to easily gain access to an individual's bank website login information, as well as logins to other websites.

Recommendations

We recommend that the Director of BEP do the following:

5. Review and enhance existing vulnerability assessment procedures to better ensure critical risks are tracked and remediated.

Management Response

BEP management stated that it will review and enhance existing vulnerability assessment procedures to better track and mitigate critical risks.

OIG Comment

Management's planned corrective action is responsive to our recommendation. However, BEP management will need to establish a definitive date that this planned action is expected to be completed in JAMES.

6. Review and enhance baseline security configuration policies to provide for more effective security settings, including those related to removable media.

Management Response

BEP management stated that it documented configuration baselines for supporting USB-cameras, and will review its policies to determine where better documentation would be appropriate.

OIG Comment

Management's planned corrective actions are responsive to our recommendation. However, BEP management will need to establish a definitive date that this planned action is expected to be completed in JAMES.

7. Ensure full disk encryption is implemented on all BEP desktops.

Management Response

BEP management stated that full disk encryption on BEP local area network/wide area network desktops is being implemented with the Windows 7 migration. Deployment efforts are underway to complete the migration by the end of March 2012.

OIG Comment

Management's planned corrective actions are responsive to our recommendation.

8. Update the BIOS to prevent booting from alternate media without entering the BIOS password.

Management Response

BEP management stated that enhanced BIOS security on BEP local area network/wide area network desktops is being implemented with the Windows 7 migration. Deployment efforts are underway to complete the migration by the end of March 2012.

OIG Comment

Management's planned corrective actions are responsive to our recommendation.

9. Review printer configurations and disable unnecessary protocols.

Management Response

BEP management stated that it has implemented the required changes to printer configurations to disable unnecessary protocols.

OIG Comment

Management's reported corrective actions are responsive to our recommendation.

10. Change default passwords on all BEP Oracle servers.

Management Response

BEP management stated that it has implemented the required changes to Oracle servers.

OIG Comment

Management's reported corrective actions are responsive to our recommendation.

11. Replace internal systems' certificates with those that meet Federal Information Processing Standards, and review internal systems to determine whether HTTPS should be enabled.

Management Response

BEP management stated that based on the recommendation and findings, BEP has initiated a re-review of the HTTPS control usage on the internal network to identify if changes are required for specific systems. This review is being factored into each systems standard certification and accreditation review process as an ongoing effort.

OIG Comment

Management's corrective actions are responsive to our recommendation. We would like to emphasize that BEP will need to replace internal systems' certificates with those that meet Federal Information Processing Standards. BEP management will also need to establish a definitive date that this planned action is expected to be completed in JAMES.

Finding 4 Public-Facing Websites Did Not Fully Comply With OMB M-10-22

We found that the privacy policy statement posted on BEP's public-facing websites MoneyFactory.gov,[9] NewMoney.gov[10] and MoneyFactoryStore.gov,[11] did not fully comply with OMB Memorandum M-10-22, "Guidance for Online Use of Web Measurement and Customization Technologies." OMB M-10-22 places requirements on federal websites that use cookies, focusing on privacy policies. The goal is to respect and safeguard the privacy of the American public while allowing the Government to improve and modernize its online operations by using cookies, a practice that had been prohibited by a previous OMB memorandum.

We found that BEP used cookies without publishing the notifications of data usage and safeguards for the privacy of its users as required by OMB M-10-22. In addition, the open government pages linked on the three websites did not provide sufficient privacy information, or publish the results of annual reviews of compliance with OMB M-10-22 and provide a means for the public to provide feedback on the results of those reviews as required.

BEP managers told us that they were not aware of the presence of the cookies because they did not request cookies from the website hosting contractor. Regardless, BEP is responsible for complying with the OMB guidance relating to the safeguarding of the American public's privacy.

[9] http://www.MoneyFactory.gov is an alias for http://www.bep.gov and is the main public website for the Bureau of Engraving and Printing.

[10] http://www.NewMoney.gov is a website whose content is centered on familiarizing various interest groups and the public in general, about the new $100 note.

[11] http://www.MoneyFactoryStore.gov is the BEP's online store, selling currency-related items to the public.

Recommendations

We recommend that the Director of BEP do the following:

12. Ensure the privacy policy statement for BEP’s public-facing websites include all elements required by OMB M-10-22.

Management Response

BEP management stated that BEP's privacy statements describe the web measurement and cookie use for the sites. BEP is working to reorganize the information presented to clearly demonstrate compliance with all elements required by OMB M-10-22. The updated privacy policies will be deployed once approved, but no later than the end of the calendar year 2011.

OIG Comment

Management’s planned corrective actions are responsive to our recommendation.

13. Perform annual reviews of BEP public-facing websites for compliance with OMB M-10-22 and report the results on the “/open” webpage of the websites.

Management Response

BEP management stated OMB M-10-22 does not require "/open" webpages on each website. The directive requires "/open" webpages on the Agency's website. For BEP, Treasury’s website satisfied this requirement, since it has and maintains the “/open” reports required by OMB M-10-22. BEP maintains open communication with Treasury’s Privacy Office to coordinate any required reporting requirements. To date, Treasury made no official request from BEP to publish specific reports on the "/open" webpages. BEP continues to work with Treasury to ensure compliance with OMB directives.

OIG Comment

Management's response meets the intent of our recommendation. We contacted the Office of Privacy, Transparency and Records

(OPTR) seeking its response on BEP's comment regarding the "/open" web pages issue. OPTR management informed us that they did not initiate "open" web pages review and, therefore, had not posted any verification results on the Treasury's "/open" page. OPTR stated that intends to move forward with this in the near future, in coordination with the Treasury Office of the Chief Information Officer (OCIO). Specifically, the Treasury OCIO is revising the current directive, TD 81-08, Certification Process for the Use of Persistent Cookies on Treasury Web Sites, to incorporate OMB Memoranda M-10-22 and M-10-23. It is anticipated that OPTR and Treasury OCIO staff will jointly initiate the review requirement in FY 2012, after which the results will be posted.

* * * * * *

I would like to extend my appreciation to the Director of BEP and his staff for the cooperation and courtesies extended to my staff during the audit. If you have any questions, please contact me at (202) 927-5171 or Abdirahman M. Salah, IT Audit Manager, at (202) 927-5763. Major contributors to this report are listed in appendix 4.

/s/

Tram Jacquelyn Dang
Audit Director

The objective of this audit was to determine whether sufficient protections were in place to prevent and detect intrusions into the Bureau of Engraving and Printing's (BEP) networks and systems. This audit is included in the *Office of Inspector General Annual Plan for 2010*.

To accomplish our objective, we utilized specialized software to conduct our vulnerability assessment, penetration test, internet-facing websites assessment, and social engineering. Specifically, we performed the following:

- We completed the vulnerability assessment and penetration tests inside BEP's network from an insider perspective with full knowledge of BEP and system access.

- We used statistical sampling to analyze the missing critical patches in desktop and server systems identified by our network vulnerability scans. We reviewed a random sample of 55 of the 220 missing critical desktop patches and 50 of the 152 missing critical server patches for the dates they were issued. We found that 33 of 55 (60 percent) missing critical desktop patches and 25 of 50 (50 percent) missing critical server patches were over 365 days old. This result was represented by a confidence level of 95 percent a sample precision of 5 percent, and expected error rate of 5 percent.

- For BEP's internet-facing websites that were external to BEP's network, we only used information available to the general public.

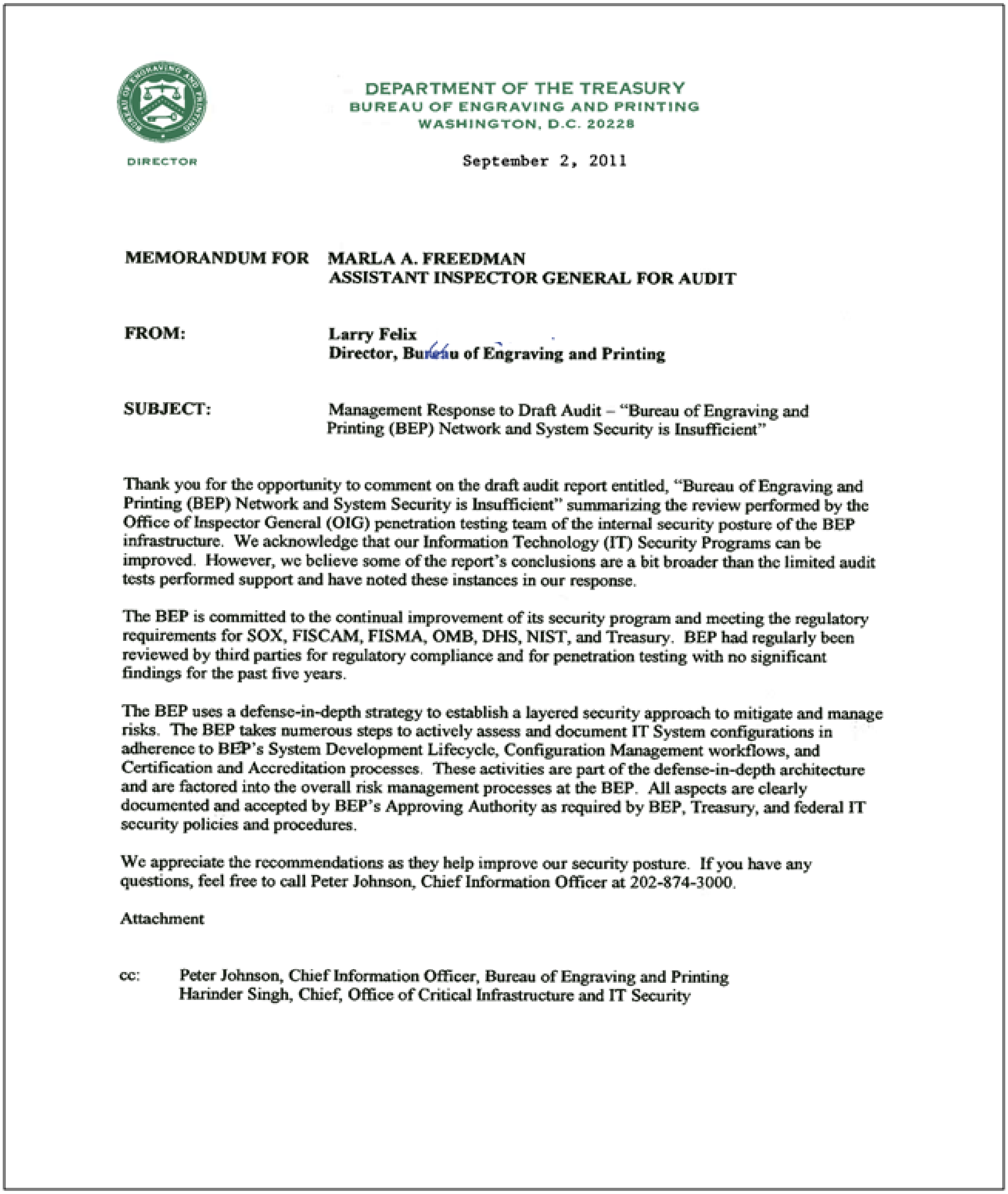
- We performed a social engineering test to determine whether BEP users were aware of cybersecurity threats or understood their roles in protecting agency information technology resources.

- We reviewed and analyzed documents related to BEP's network and systems, and interviewed BEP information technology security and operations personnel.

We performed our fieldwork at BEP headquarters location in Washington, DC, from May 2010 through April 2011. Upon completion of our tests, we provided BEP's Chief Information

Officer staff with the reports generated by our automated assessment tools in July 2010, so that timely corrective actions could be taken. The reports provided details on specific vulnerabilities detected and exploited, and the suggested actions necessary to address them. We also provided BEP management with Notifications of Findings and Recommendations along with our analysis of the issues reported by the tools we used. The results of this audit may be used to support our work undertaken in accordance with the requirements of the Federal Information Security Management Act.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to prove a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.



DEPARTMENT OF THE TREASURY
BUREAU OF ENGRAVING AND PRINTING
WASHINGTON, D.C. 20228

DIRECTOR

September 2, 2011

MEMORANDUM FOR **MARLA A. FREEDMAN**
ASSISTANT INSPECTOR GENERAL FOR AUDIT

FROM: **Larry Felix**
Director, Bureau of Engraving and Printing

SUBJECT: Management Response to Draft Audit – "Bureau of Engraving and Printing (BEP) Network and System Security is Insufficient"

Thank you for the opportunity to comment on the draft audit report entitled, "Bureau of Engraving and Printing (BEP) Network and System Security is Insufficient" summarizing the review performed by the Office of Inspector General (OIG) penetration testing team of the internal security posture of the BEP infrastructure. We acknowledge that our Information Technology (IT) Security Programs can be improved. However, we believe some of the report's conclusions are a bit broader than the limited audit tests performed support and have noted these instances in our response.

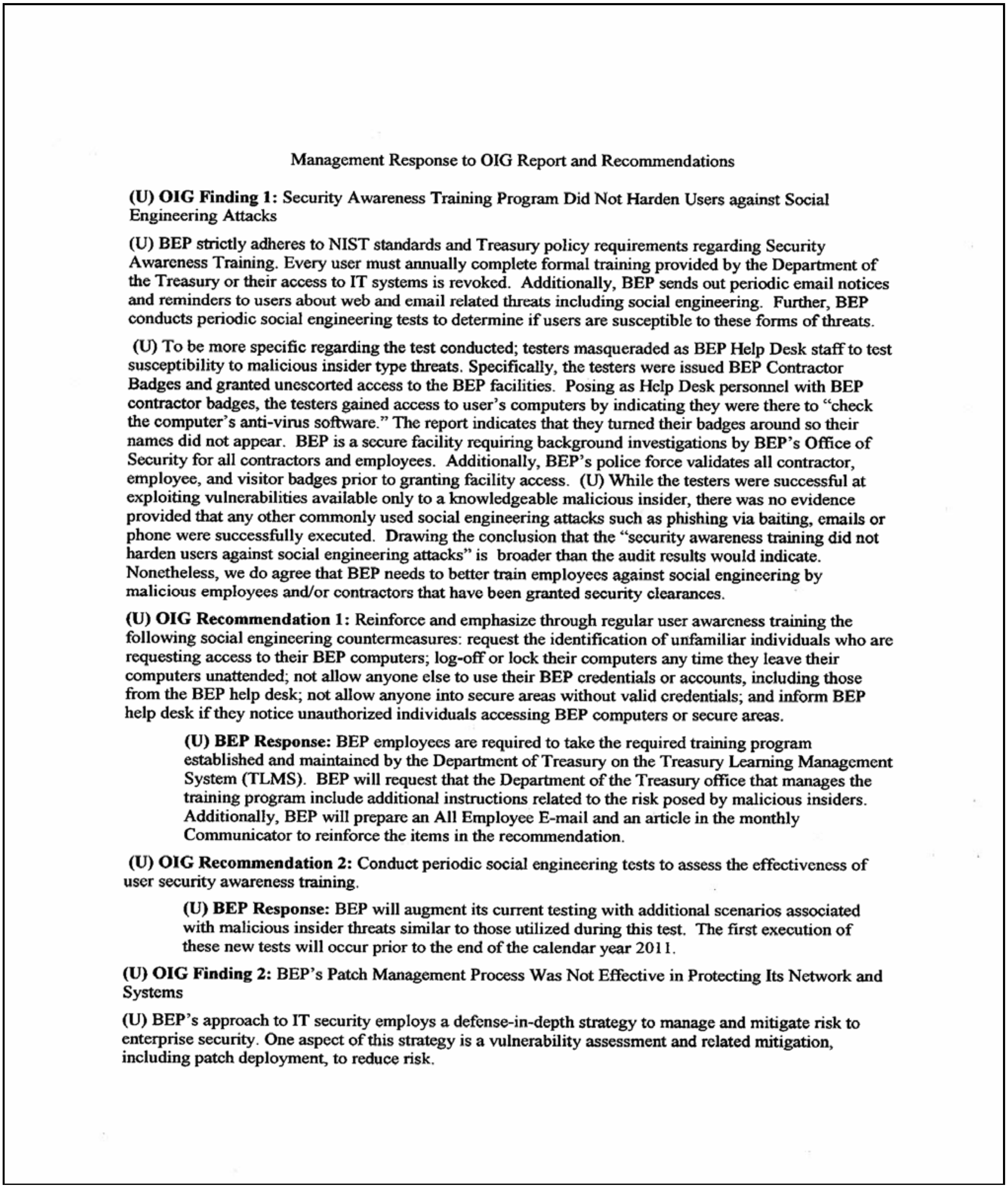
The BEP is committed to the continual improvement of its security program and meeting the regulatory requirements for SOX, FISCAM, FISMA, OMB, DHS, NIST, and Treasury. BEP had regularly been reviewed by third parties for regulatory compliance and for penetration testing with no significant findings for the past five years.

The BEP uses a defense-in-depth strategy to establish a layered security approach to mitigate and manage risks. The BEP takes numerous steps to actively assess and document IT System configurations in adherence to BEP's System Development Lifecycle, Configuration Management workflows, and Certification and Accreditation processes. These activities are part of the defense-in-depth architecture and are factored into the overall risk management processes at the BEP. All aspects are clearly documented and accepted by BEP's Approving Authority as required by BEP, Treasury, and federal IT security policies and procedures.

We appreciate the recommendations as they help improve our security posture. If you have any questions, feel free to call Peter Johnson, Chief Information Officer at 202-874-3000.

Attachment

cc: Peter Johnson, Chief Information Officer, Bureau of Engraving and Printing
Harinder Singh, Chief, Office of Critical Infrastructure and IT Security



Management Response to OIG Report and Recommendations

(U) OIG Finding 1: Security Awareness Training Program Did Not Harden Users against Social Engineering Attacks

(U) BEP strictly adheres to NIST standards and Treasury policy requirements regarding Security Awareness Training. Every user must annually complete formal training provided by the Department of the Treasury or their access to IT systems is revoked. Additionally, BEP sends out periodic email notices and reminders to users about web and email related threats including social engineering. Further, BEP conducts periodic social engineering tests to determine if users are susceptible to these forms of threats.

(U) To be more specific regarding the test conducted; testers masqueraded as BEP Help Desk staff to test susceptibility to malicious insider type threats. Specifically, the testers were issued BEP Contractor Badges and granted unescorted access to the BEP facilities. Posing as Help Desk personnel with BEP contractor badges, the testers gained access to user's computers by indicating they were there to "check the computer's anti-virus software." The report indicates that they turned their badges around so their names did not appear. BEP is a secure facility requiring background investigations by BEP's Office of Security for all contractors and employees. Additionally, BEP's police force validates all contractor, employee, and visitor badges prior to granting facility access. (U) While the testers were successful at exploiting vulnerabilities available only to a knowledgeable malicious insider, there was no evidence provided that any other commonly used social engineering attacks such as phishing via baiting, emails or phone were successfully executed. Drawing the conclusion that the "security awareness training did not harden users against social engineering attacks" is broader than the audit results would indicate. Nonetheless, we do agree that BEP needs to better train employees against social engineering by malicious employees and/or contractors that have been granted security clearances.

(U) OIG Recommendation 1: Reinforce and emphasize through regular user awareness training the following social engineering countermeasures: request the identification of unfamiliar individuals who are requesting access to their BEP computers; log-off or lock their computers any time they leave their computers unattended; not allow anyone else to use their BEP credentials or accounts, including those from the BEP help desk; not allow anyone into secure areas without valid credentials; and inform BEP help desk if they notice unauthorized individuals accessing BEP computers or secure areas.

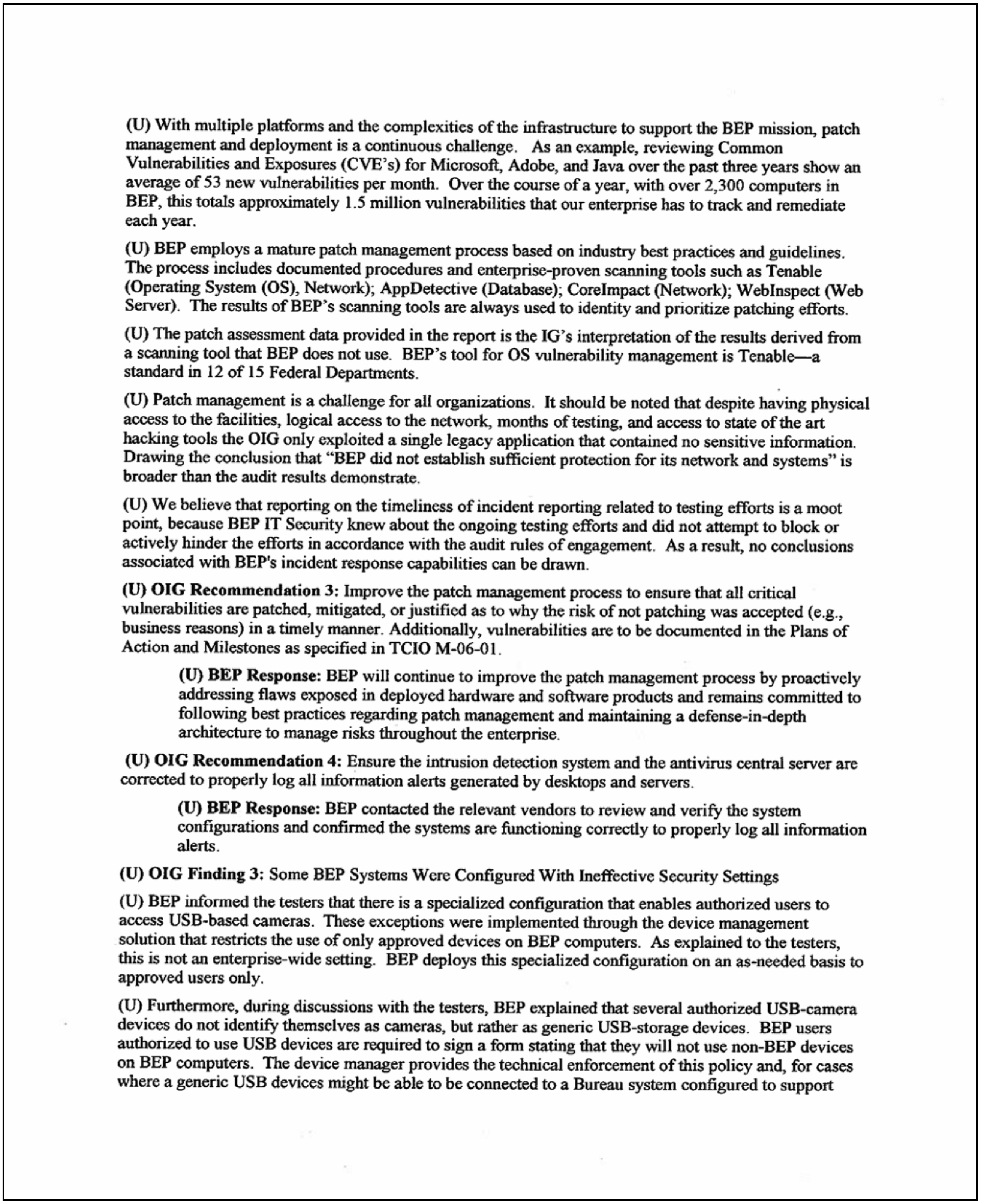
> **(U) BEP Response:** BEP employees are required to take the required training program established and maintained by the Department of Treasury on the Treasury Learning Management System (TLMS). BEP will request that the Department of the Treasury office that manages the training program include additional instructions related to the risk posed by malicious insiders. Additionally, BEP will prepare an All Employee E-mail and an article in the monthly Communicator to reinforce the items in the recommendation.

(U) OIG Recommendation 2: Conduct periodic social engineering tests to assess the effectiveness of user security awareness training.

> **(U) BEP Response:** BEP will augment its current testing with additional scenarios associated with malicious insider threats similar to those utilized during this test. The first execution of these new tests will occur prior to the end of the calendar year 2011.

(U) OIG Finding 2: BEP's Patch Management Process Was Not Effective in Protecting Its Network and Systems

(U) BEP's approach to IT security employs a defense-in-depth strategy to manage and mitigate risk to enterprise security. One aspect of this strategy is a vulnerability assessment and related mitigation, including patch deployment, to reduce risk.



(U) With multiple platforms and the complexities of the infrastructure to support the BEP mission, patch management and deployment is a continuous challenge. As an example, reviewing Common Vulnerabilities and Exposures (CVE's) for Microsoft, Adobe, and Java over the past three years show an average of 53 new vulnerabilities per month. Over the course of a year, with over 2,300 computers in BEP, this totals approximately 1.5 million vulnerabilities that our enterprise has to track and remediate each year.

(U) BEP employs a mature patch management process based on industry best practices and guidelines. The process includes documented procedures and enterprise-proven scanning tools such as Tenable (Operating System (OS), Network); AppDetective (Database); CoreImpact (Network); WebInspect (Web Server). The results of BEP's scanning tools are always used to identity and prioritize patching efforts.

(U) The patch assessment data provided in the report is the IG's interpretation of the results derived from a scanning tool that BEP does not use. BEP's tool for OS vulnerability management is Tenable—a standard in 12 of 15 Federal Departments.

(U) Patch management is a challenge for all organizations. It should be noted that despite having physical access to the facilities, logical access to the network, months of testing, and access to state of the art hacking tools the OIG only exploited a single legacy application that contained no sensitive information. Drawing the conclusion that "BEP did not establish sufficient protection for its network and systems" is broader than the audit results demonstrate.

(U) We believe that reporting on the timeliness of incident reporting related to testing efforts is a moot point, because BEP IT Security knew about the ongoing testing efforts and did not attempt to block or actively hinder the efforts in accordance with the audit rules of engagement. As a result, no conclusions associated with BEP's incident response capabilities can be drawn.

(U) OIG Recommendation 3: Improve the patch management process to ensure that all critical vulnerabilities are patched, mitigated, or justified as to why the risk of not patching was accepted (e.g., business reasons) in a timely manner. Additionally, vulnerabilities are to be documented in the Plans of Action and Milestones as specified in TCIO M-06-01.

> **(U) BEP Response:** BEP will continue to improve the patch management process by proactively addressing flaws exposed in deployed hardware and software products and remains committed to following best practices regarding patch management and maintaining a defense-in-depth architecture to manage risks throughout the enterprise.

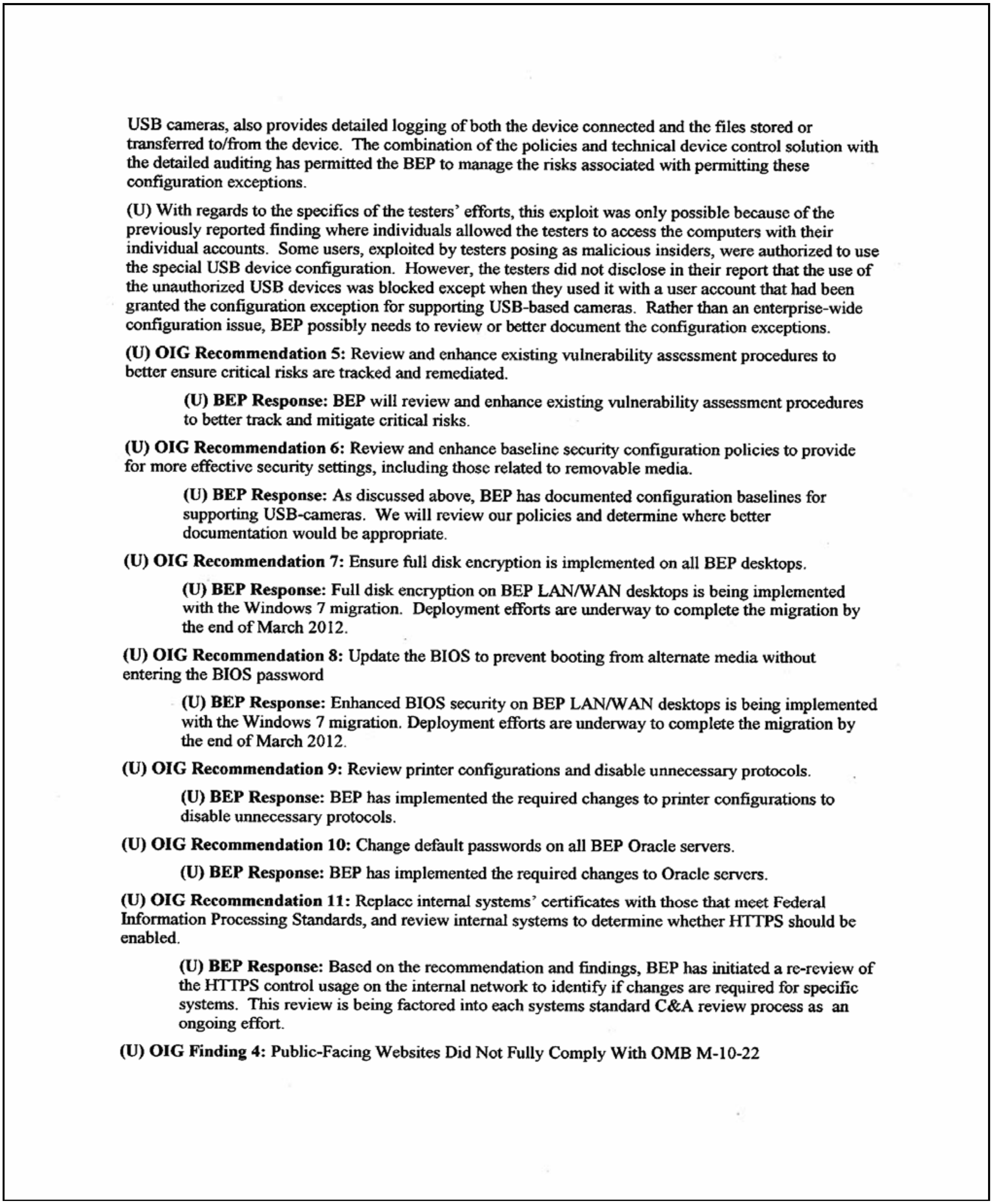
(U) OIG Recommendation 4: Ensure the intrusion detection system and the antivirus central server are corrected to properly log all information alerts generated by desktops and servers.

> **(U) BEP Response:** BEP contacted the relevant vendors to review and verify the system configurations and confirmed the systems are functioning correctly to properly log all information alerts.

(U) OIG Finding 3: Some BEP Systems Were Configured With Ineffective Security Settings

(U) BEP informed the testers that there is a specialized configuration that enables authorized users to access USB-based cameras. These exceptions were implemented through the device management solution that restricts the use of only approved devices on BEP computers. As explained to the testers, this is not an enterprise-wide setting. BEP deploys this specialized configuration on an as-needed basis to approved users only.

(U) Furthermore, during discussions with the testers, BEP explained that several authorized USB-camera devices do not identify themselves as cameras, but rather as generic USB-storage devices. BEP users authorized to use USB devices are required to sign a form stating that they will not use non-BEP devices on BEP computers. The device manager provides the technical enforcement of this policy and, for cases where a generic USB devices might be able to be connected to a Bureau system configured to support



USB cameras, also provides detailed logging of both the device connected and the files stored or transferred to/from the device. The combination of the policies and technical device control solution with the detailed auditing has permitted the BEP to manage the risks associated with permitting these configuration exceptions.

(U) With regards to the specifics of the testers' efforts, this exploit was only possible because of the previously reported finding where individuals allowed the testers to access the computers with their individual accounts. Some users, exploited by testers posing as malicious insiders, were authorized to use the special USB device configuration. However, the testers did not disclose in their report that the use of the unauthorized USB devices was blocked except when they used it with a user account that had been granted the configuration exception for supporting USB-based cameras. Rather than an enterprise-wide configuration issue, BEP possibly needs to review or better document the configuration exceptions.

(U) OIG Recommendation 5: Review and enhance existing vulnerability assessment procedures to better ensure critical risks are tracked and remediated.

> **(U) BEP Response:** BEP will review and enhance existing vulnerability assessment procedures to better track and mitigate critical risks.

(U) OIG Recommendation 6: Review and enhance baseline security configuration policies to provide for more effective security settings, including those related to removable media.

> **(U) BEP Response:** As discussed above, BEP has documented configuration baselines for supporting USB-cameras. We will review our policies and determine where better documentation would be appropriate.

(U) OIG Recommendation 7: Ensure full disk encryption is implemented on all BEP desktops.

> **(U) BEP Response:** Full disk encryption on BEP LAN/WAN desktops is being implemented with the Windows 7 migration. Deployment efforts are underway to complete the migration by the end of March 2012.

(U) OIG Recommendation 8: Update the BIOS to prevent booting from alternate media without entering the BIOS password

> **(U) BEP Response:** Enhanced BIOS security on BEP LAN/WAN desktops is being implemented with the Windows 7 migration. Deployment efforts are underway to complete the migration by the end of March 2012.

(U) OIG Recommendation 9: Review printer configurations and disable unnecessary protocols.

> **(U) BEP Response:** BEP has implemented the required changes to printer configurations to disable unnecessary protocols.

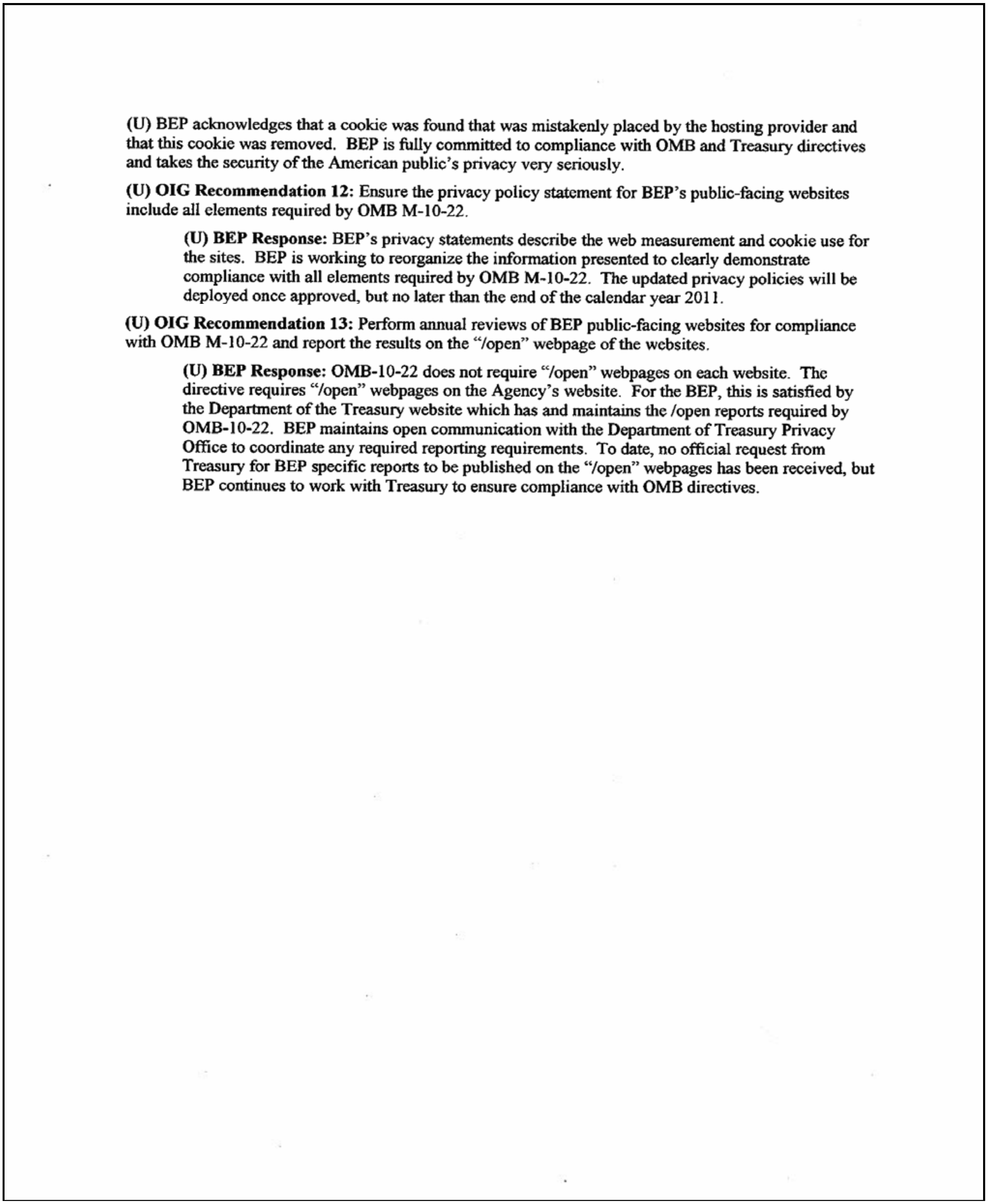
(U) OIG Recommendation 10: Change default passwords on all BEP Oracle servers.

> **(U) BEP Response:** BEP has implemented the required changes to Oracle servers.

(U) OIG Recommendation 11: Replace internal systems' certificates with those that meet Federal Information Processing Standards, and review internal systems to determine whether HTTPS should be enabled.

> **(U) BEP Response:** Based on the recommendation and findings, BEP has initiated a re-review of the HTTPS control usage on the internal network to identify if changes are required for specific systems. This review is being factored into each systems standard C&A review process as an ongoing effort.

(U) OIG Finding 4: Public-Facing Websites Did Not Fully Comply With OMB M-10-22



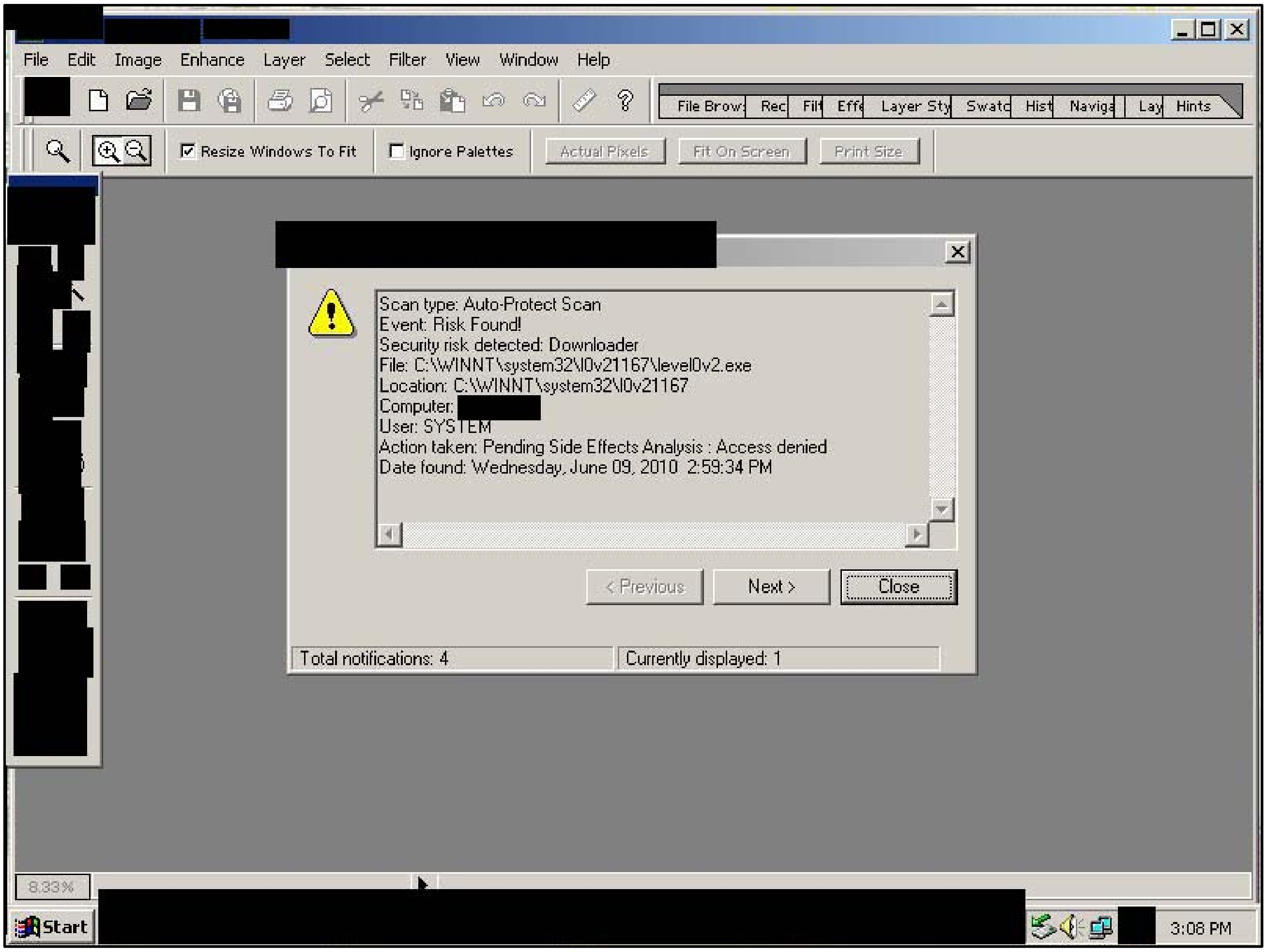
(U) BEP acknowledges that a cookie was found that was mistakenly placed by the hosting provider and that this cookie was removed. BEP is fully committed to compliance with OMB and Treasury directives and takes the security of the American public's privacy very seriously.

(U) OIG Recommendation 12: Ensure the privacy policy statement for BEP's public-facing websites include all elements required by OMB M-10-22.

> **(U) BEP Response:** BEP's privacy statements describe the web measurement and cookie use for the sites. BEP is working to reorganize the information presented to clearly demonstrate compliance with all elements required by OMB M-10-22. The updated privacy policies will be deployed once approved, but no later than the end of the calendar year 2011.

(U) OIG Recommendation 13: Perform annual reviews of BEP public-facing websites for compliance with OMB M-10-22 and report the results on the "/open" webpage of the websites.

> **(U) BEP Response:** OMB-10-22 does not require "/open" webpages on each website. The directive requires "/open" webpages on the Agency's website. For the BEP, this is satisfied by the Department of the Treasury website which has and maintains the /open reports required by OMB-10-22. BEP maintains open communication with the Department of Treasury Privacy Office to coordinate any required reporting requirements. To date, no official request from Treasury for BEP specific reports to be published on the "/open" webpages has been received, but BEP continues to work with Treasury to ensure compliance with OMB directives.

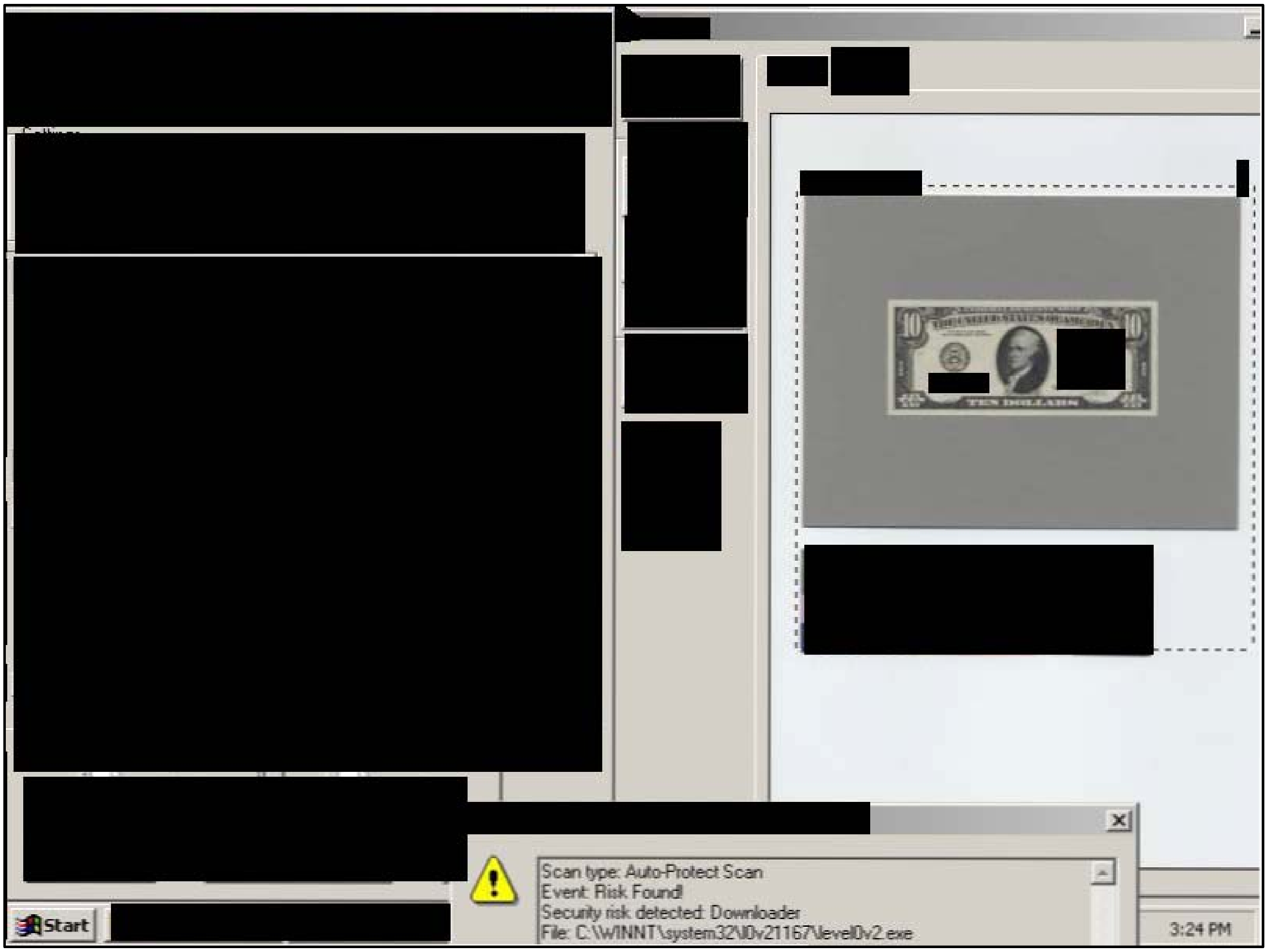


[redacted]

Scan type: Auto-Protect Scan
Event: Risk Found!
Security risk detected: Downloader
File: C:\WINNT\system32\l0v21167\level0v2.exe
Location: C:\WINNT\system32\l0v21167
Computer: [redacted]
User: SYSTEM
Action taken: Pending Side Effects Analysis : Access denied
Date found: Wednesday, June 09, 2010 2:59:34 PM

Total notifications: 4
Currently displayed: 1

Appendix 3
Screenshots of Real-Time BEP User Activity



[redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted]

Scan type: Auto-Protect Scan
Event: Risk Found!
Security risk detected: Downloader
File: C:\WINNT\system32\l0v21167\level0v2.exe

Office of Information Technology (IT) Audit

Tram J. Dang, Audit Director
Abdirahman M. Salah, IT Audit Manager
Kevin Mfume, IT Specialist
Yeshorohan K. Mandadi, IT Specialist
Daniel A. Jensen, IT Specialist
Gerald Kelly, Referencer

Department of the Treasury

Office of the Chief Information Officer
Office of Accounting and Internal Control
Office of Strategic Planning and Performance Management

Office of Management and Budget

Office of Inspector General Budget Examiner