



Audit Report



OIG-17-007

INFORMATION TECHNOLOGY: Fiscal Service Needs to Strengthen Security Controls over Public-Facing Web Servers

November 14, 2016

Office of
Inspector General

Department of the Treasury

Contents

Audit Report

Results in Brief	2
Background	3
Results of Audit	4
Local Administrative Accounts Were Managed Poorly	4
Recommendation	5
Unauthorized Software Was Present	5
Recommendations	6
Configuration Scans Used Unapproved Baselines	7
Recommendation	8
Operating Systems Were Obsolete	8
Recommendation	9
Ethicsburg Website Was Vulnerable to Cross-Site Scripting Attacks	9
Recommendation	10
Sensitive Information Was Revealed In Error Messages	11
Recommendation	11
Security Procedures Were Not Documented	12
Recommendation	13

Appendices

Appendix 1 Objective, Scope, and Methodology	14
Appendix 2 Management Response	15
Appendix 3 Major Contributors to This Report	19
Appendix 4 Report Distribution	20

Abbreviations

ARC	Administrative Resource Center
EITI	Enterprise Information Technology Infrastructure
FISMA	Federal Information Security Modernization Act of 2014
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
SP	Special Publication
SSP	System Security Plan

*The Department of the Treasury
Office of Inspector General*

November 14, 2016

Sheryl Morrow
Commissioner, Bureau of the Fiscal Service

This report represents the results of our audit of the security controls over public-facing web servers used by the Bureau of the Fiscal Service (Fiscal Service). We performed this audit as part of our ongoing oversight of the Department of the Treasury's (Treasury) compliance with the *Federal Information Security Modernization Act of 2014* (FISMA), which requires Federal agencies to provide adequate information security for networks, facilities, and systems or groups of information systems, as appropriate. In this regard, we perform periodic audits of networks and information security of Treasury bureaus and offices. The overall objective of this audit was to assess whether effective security controls were in place to protect Fiscal Service's public-facing web servers. Fiscal Service was selected for audit because it had more websites hosted on public-facing web servers than any other Department of the Treasury bureau or office.

To accomplish our audit objective, we reviewed the inventory of public-facing web servers operated by Treasury's bureaus and offices to assess how servers had been implemented; interviewed personnel at Fiscal Service; reviewed and analyzed security-related documentation; and observed security control configurations demonstrated by technical personnel. Appendix 1 provides more detail on our objective, scope, and methodology.

Results in Brief

We identified seven findings in Fiscal Service's security controls over public-facing web servers. Specifically, we found the following:

- Local administrative accounts were managed poorly and not in accordance with Fiscal Service policies. Management did not ensure that administrative accounts that were no longer needed were removed from the six servers in our sample. That is, 65 of the 141 active accounts with local administrative privileges should not have been active.
- Fiscal Service had unauthorized software installed on its public-facing web servers. Some installed software, such as administrative tools and multiple versions of web server software, were missing from their approved software list.
- Staff performed regular compliance scans against configuration baselines that were not approved by management. Furthermore, management could not provide evidence of review and approval of configuration baselines between April 2013 and June 2015, and did not have a list of approved baseline deviations for the public-facing web servers selected in our sample.
- Some operating systems used for public-facing web servers were running Microsoft Windows Server 2003, which had not been supported by Microsoft since July 2015. Therefore, security updates have not been released by Microsoft since that date.
- One website was vulnerable to cross-site scripting attacks¹ because it did not validate input received from user's webpage requests. This allowed us to create and send webpage requests that resulted in a cross-site scripting proof-of-concept attack, which opened a pop-up window in the user's browser.

¹ Cross-site scripting is an attack using a browser-side scripting language, often JavaScript. The goal of the attacker is to make malicious script appear to be from a site trusted by the user being attacked, so the user's browser would not identify the script being executed is not meant to be part of the site they are viewing.

-
- An Administrative Resource Center (ARC) public-facing website was configured to display error messages that revealed the web server version number and the operating system. This information provides leads for attackers to exploit to specific software vulnerabilities.
 - Security procedures were not documented for access control, identification and authentication, system and communications protection, and system and information integrity for public-facing servers.

Accordingly, we are making eight recommendations to management to address the deficiencies identified.

In a written response, management agreed with our findings and recommendations, and stated that remediation plans to address the deficiencies identified in this report have been developed along with targeted implementation dates. Overall, we found that management's response meets the intent of our recommendations. We have summarized and evaluated management's response in the recommendation sections of this report. Management's response is provided in appendix 2.

Background

The Federal government develops and maintains over 1,000 publicly accessible websites in order to share information, collaborate and conduct business with the public and business partners, and provide employees and contractors with remote access to their networks. Public-facing servers are accessible to anyone with an Internet connection, and as such, vulnerabilities in those servers may introduce risks to the network and systems of Treasury bureaus and offices.

Fiscal Service's mission is to promote the financial integrity and operational efficiency of the Federal government through accounting, financing, collections, payments, and shared services. Fiscal Service maintains public-facing web servers to host websites and web applications in support of that mission. Because Fiscal Service's public-facing web servers are connected to its network, other bureaus' networks, and the Internet, it is important that those servers have sufficiently secure configurations and controls. Additionally, FISMA requires

Federal agencies to provide adequate information security for networks, facilities, and systems or groups of information systems, as appropriate.

Results of Audit

Finding 1 **Local Administrative Accounts Were Managed Poorly**

Local administrative accounts on Fiscal Service's public-facing web servers were not managed in accordance with Fiscal Service policies. Fiscal Service management did not ensure that administrative accounts that were no longer needed were removed from the six servers in our sample. That is, 65 of the 141 active accounts with local administrative privileges should not have been active. Specifically, we found 27 accounts belonged to users who no longer needed access and 38 accounts were not certified or approved to have administrative privileges. In addition, we found 9 accounts did not follow Fiscal Service's naming scheme.

The National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, requires organizations to manage information system accounts, including deactivating accounts of terminated or transferred users, and reviewing accounts at a frequency defined by the organization. Fiscal Service's *Enterprise Information Technology Infrastructure (EITI) System Security Plan (SSP)*, dated February 2014, requires staff to review privileged accounts at least once within each calendar half year.

According to a representative of the Identity Administration Branch, Fiscal Service's manual processes for managing and recertifying local privileged accounts were the reason for accounts not being properly managed. When asked, management did not provide the dates when these accounts should have been disabled, modified, or removed.

Local administrative accounts that are not timely removed when no longer needed provide opportunities for unfettered access to Fiscal Service's public facing servers and can result in unauthorized modification, deletion, or retrieval of information and system files. Even when compensating controls prevent the original account holder from logging in, unattended active

administrative accounts are attractive targets for hackers to access and exploit servers. Unauthorized activities from these privileged accounts could possibly go undetected, as the actions are originating from what appears to be an authorized source.

Recommendation

1. We recommend that the Commissioner of the Bureau of the Fiscal Service ensure all user accounts are regularly reviewed and removed in accordance with NIST SP 800-53 and Fiscal Service policies and procedures.

Management Response

Management agreed with our recommendation and reported that Fiscal Service has removed the inactive accounts. Management further stated that it will ensure processes are in place to regularly review and remove user accounts that are no longer required on public-facing web servers. This action has a target completion date of June 30, 2017.

OIG Comment

Management's reported and planned corrective actions meet the intent of our recommendation.

Finding 2 Unauthorized Software Was Present

Unapproved software was installed on Fiscal Service's public-facing web servers. Specifically, we found 12 installed programs, such as administrative tools and multiple versions of web server software, were missing from their approved software list.

NIST SP 800-53, Revision 4, requires organizations to maintain a "blacklist" of software not permitted on a moderate impact system. Fiscal Service uses the approved software list as a "whitelist," a more stringent control that specifies the software permitted on its systems. Furthermore, Treasury Directive Publication 85-01, *Treasury Information Technology Security Program*, requires the heads of Bureaus and Offices to establish and maintain an accurate software inventory and conduct software inventory reviews.

A representative from the Division of Service Management told us that Fiscal Service did not have a comprehensive software asset management program in place to compare servers against the approved list. Without an effective software asset management program, software that is not approved may be present on the system. Information technology staff might not manage unapproved software, which would increase the likelihood of information security breaches due to unpatched vulnerabilities and malicious codes. Further, unapproved software could be unlicensed, increasing the risk of violation of software licensing terms.

Recommendations

We recommend that the Commissioner of the Bureau of the Fiscal Service do the following:

2. Establish and maintain a software asset management program to ensure that only approved software is installed on public-facing web servers.

Management Response

Management agreed with our recommendation and stated that Fiscal Service currently manages a software asset management program that periodically scans for software that is hosted on Fiscal Service data center assets, including public-facing websites. This program includes the identification of the application and authorized licensing for those assets. In concert with the periodic update of the Approved Product List, any authorized software is identified and designated for removal from any server in the Fiscal IT infrastructure. Fiscal Service will validate the effectiveness of the software asset management program by February 28, 2017.

OIG Comment

Management's planned corrective actions meet the intent of our recommendation.

3. Remove software that is not approved from public-facing web servers.

Management Response

Management agreed with our recommendation and reported that Fiscal Service will remove any unauthorized software, as described in management response under Recommendation 2, by February 28, 2017.

OIG Comment

Management's planned corrective actions meet the intent of our recommendation.

Finding 3 Configuration Scans Used Unapproved Baselines

We found deficiencies in Fiscal Service's configuration baseline management. Specifically, Fiscal Service's Threat Management Team performed regular compliance scans against configuration baselines that were not approved by management. Furthermore, management could not provide evidence of review and approval of configuration baselines between April 2013 and June 2015. Lastly, Fiscal Service did not have a list of approved baseline deviations for the public-facing web servers selected in our sample.

NIST SP 800-53, Rev. 4, requires that organizations develop, document, and maintain under configuration control, a current baseline configuration of the information system. Fiscal Service's EITI SSP, requires that the organization review and update baseline configurations annually. In addition, NIST SP 800-53, Rev. 4, requires organizations to document and approve deviations from established configuration settings for certain information system components based on operational requirements.

According to a representative from the Enterprise Cyber Security Division, there was no centralized process for submission, review, approval, and storage of security baselines. Using incorrect or unapproved configuration baselines increases the risk of insecure configuration settings for the systems, increasing the risk of being compromised or misused. If configuration baselines are not reviewed and approved by management, staff and management across organization could use incorrect or unapproved baselines. Without a documented and approved list of baseline deviations, systems may be

configured with unsecured settings without management's knowledge.

Recommendation

4. We recommend that the Commissioner of the Bureau of the Fiscal Service establish a centralized process for submission, review, approval, storage, and management of security baselines and deviations that is consistent with the EITI SSP.

Management Response

Management agreed with our recommendation and reported that Fiscal Service will establish a centralized process for submission, review, approval, storage, and management of security baselines and deviations that is consistent with the EITI SSP. Management further stated that Fiscal Service has archived outdated files and created a new document set which contains current baselines and submission dates. These dates will be used to monitor the files and notify appropriate personnel when the document approaches its annual renewal date. Procedures for documenting baseline deviations are in draft form and will be implemented by January 31, 2017.

OIG Comment

Management's planned corrective actions meet the intent of our recommendation.

Finding 4 Operating Systems Were Obsolete

We found 2 of 6 public-facing web servers tested were running Microsoft Windows Server 2003, which had not been supported by Microsoft since July 2015. Therefore, security updates have not been released by Microsoft since that date.

NIST SP 800-53, Rev. 4, requires organizations to correct information system flaws and install security-relevant software updates and patches. Additionally, Fiscal Service's EITI SSP requires that security-relevant software and firmware updates be installed within 90 days of release.

A representative from the Windows Engineering Branch did not provide us with the reasons for the public-facing web servers in question running obsolete software, but stated that these

servers belong to Customer General Application Team. However, we could not attribute responsibility for updating the operating system to either group. He also mentioned that waiver forms were being developed. Waiver forms can be used to document acceptance of risk posed by security risks such as obsolete operating systems. However, 6 months had already passed the end of support for Windows Server 2003 at the time of our inquiry without the risk having been formally accepted in a signed waiver or other document acknowledging and accepting risk.

Operating systems that are no longer supported will not receive patches from the vendor and remain vulnerable to any newly discovered security flaws.

Recommendation

5. We recommend that the Commissioner of the Bureau of the Fiscal Service ensure that public-facing web servers are running supported operating systems so that updates are timely applied.

Management Response

Management agreed with our recommendation and stated that Fiscal Service recognizes the importance of hosting services on supported operating systems. Management further reported that it will complete the ongoing effort to upgrade any remaining obsolete systems and implement a process to proactively prevent the hosting of applications on obsolete/unsupported operating systems by March 31, 2017.

OIG Comment

Management's planned corrective actions meet the intent of our recommendation.

Finding 5 Ethicsburg Website Was Vulnerable to Cross-Site Scripting Attacks

We determined that the Fiscal Service's Ethicsburg² website, which provides annual ethics training to Federal employees, was vulnerable to cross-site scripting attacks because it did not

² <http://www.ethicsburg.gov>

validate input received from user's webpage requests. We were able to create and send webpage requests that resulted in a cross-site scripting proof-of-concept attack, which opened a pop-up window in the user's browser.

NIST SP 800-53, Rev. 4, requires that information systems check the validity of input to verify that it matches the expected format and content in order to prevent cross-site scripting and other injection-style attacks. According to a representative from the Division of Business Integration, Ethicsburg.gov is a minor site that was developed over a decade ago, and at the time, the concept of cross-site scripting was not an issue. Management further stated that subsequent changes in the underlying environment never necessitated a need to rewrite the site and there has not been any effort given to address changing the way the site works.

Failing to perform adequate input validation has left users who visited Ethicsburg website vulnerable to cross-site scripting attacks. As a result, attackers could get a user's browser to execute malicious code within the security context of Ethicsburg's website. With this privilege, the code has the ability to read, modify, and transmit any sensitive data accessible by the browser. Malicious scripts can redirect users to another website or possibly show fraudulent content without alerting users to the attack.

Recommendation

6. We recommend that the Commissioner of the Bureau of the Fiscal Service remediate the cross-site scripting vulnerability in the Ethicsburg web site.

Management Response

Management agreed with our recommendation and reported that Ethicsburg will be modified to ensure input validation is in place to prevent cross-site scripting. Code changes, testing, and migration to production will be completed by January 31, 2017.

OIG Comment

Management's planned corrective actions meet the intent of our recommendation.

Finding 6

Sensitive Information Was Revealed In Error Messages

Fiscal Service's Administrative Resource Center public-facing website was configured to display error messages that revealed the web server version number and the operating system. This information provides leads for attackers to exploit specific software vulnerabilities.

NIST SP 800-53, Rev. 4, requires that organizations utilize error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.

According to a representative from the Middleware Engineering Branch, Fiscal Service was aware of this weakness and support from the content management area was needed to reconfigure custom error pages on the public-facing web servers to address this issue. However, we have not seen any corrections taken, and the information remained disclosed on this website at the time of this report, more than 7 months after that response was provided.

Public-facing web servers that reveal specific software version information provide information regarding their potential vulnerabilities. If an attacker knows the exact software and version, the amount of time required for a successful attack vector to be identified and exploited can be greatly reduced.

Recommendation

7. We recommend that the Commissioner of the Bureau of the Fiscal Service ensure that public-facing web servers used by the Administrative Resource Center website are configured to prevent disclosure of sensitive system information.

Management Response

Management agreed with our recommendation and reported that Fiscal Service has taken appropriate actions to replace error messages on the ARC public-facing web servers. Management further stated that Fiscal Service will validate that any default ARC error messages generated by the hosted web service that revealed sensitive information has been remediated by January 31, 2017.

OIG Comment

Management's reported and planned corrective actions meet the intent of our recommendation.

Finding 7 Security Procedures Were Not Documented

Fiscal Service did not document security procedures for access control, identification and authentication, system and communications protection, and system and information integrity for public-facing servers. Management initially provided us with the Active Directory policies, a system logging standard operating procedure, a telephone server installation standard operating procedure, and database policies and procedures. However, we noted that these documents did not provide procedures for these security controls.

In response to our concern over the lack of documentation, a representative from the Security Policy and Risk Management Branch stated that Fiscal Service staff had not provided the correct policy and procedure documents and referred us to the "Baseline Security Requirements" document and the "Fiscal Service Information Technology Security Program Plan" for the required controls. These documents provided information on policies for information security controls, but did not include procedures sufficient to fully implement them.

NIST SP 800-53, Rev. 4, requires that organizations develop, document, and maintain policies and procedures for several aspects of information system management, including access control, identification and authentication, system and communications protection, and system and information integrity. Written procedures should support the policies and facilitate the implementation of the policies and associated controls.

If procedures are not documented, staff responsible for the implementation of security controls may not correctly apply the required settings to ensure that controls are implemented. As a result, security controls over public-facing web servers may not be properly implemented.

Recommendation

8. We recommend that the Commissioner of the Bureau of the Fiscal Service ensure that information security procedures for public-facing servers are documented.

Management Response

Management agreed with our recommendation and reported that Fiscal Service has redesigned and updated document storage procedures to address the issue of NIST SP 800-53 documentation requirements. Management further stated that Fiscal Service has implemented a new program, the "CIO Publications Library," to maintain IT, including security related procedures. This Library uses standardized document templates which include document purpose, background, related documents, scope of the document, and roles and duties assigned to personnel by the document. Management commitment is documented by requiring explicit managerial approval prior to publication of documents. Conversion of documents from the legacy IT Standards Program was completed on July 1, 2016.

OIG Comment

Management's reported and planned corrective actions meet the intent of our recommendation.

* * * * *

I would like to extend my appreciation to the Fiscal Service staff for the cooperation and courtesies extended to my staff during the audit. If you have any questions, please contact me at (202) 927-0361. Major contributors to this report are listed in appendix 3.

Larissa Klimpel
Acting Director, Cyber/Information Technology Audit

In November 2014, we initiated an audit of the security controls over public-facing web servers used by the Department of the Treasury's (Treasury) Bureau of the Fiscal Service (Fiscal Service). Our objective for this audit was to assess whether effective security controls were in place to protect Fiscal Service's public-facing web servers.

As part of the audit, we performed a Treasury-wide data call for information on public-facing websites. Based on the results, we selected Fiscal Service for this audit because Fiscal Service has more public-facing web applications as compared to Treasury's other bureaus and offices.

We selected a sample of six public-facing web servers to test based on monthly traffic, number of users, and our assessment of risk presented by selected servers. These servers were managed by Fiscal Service.

In performing our work, we interviewed personnel at Fiscal Service; reviewed applicable National Institute of Standards and Technology Special Publications, as well as Treasury's and Fiscal Service's policies and procedures; reviewed and analyzed key documents related to virtual servers; and observed remote demonstrations of security control configurations performed by Fiscal Service technical personnel. We performed our fieldwork primarily at Treasury Office of Inspector General headquarters in Washington, D.C. from November 2014 through January 2016.

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

Appendix 2
Management Response



DEPARTMENT OF THE TREASURY
BUREAU OF THE FISCAL SERVICE
WASHINGTON, DC 20227

September 2, 2016

Ms. Tram Dang
Director, IT Audit
U.S. Department of the Treasury
Office of the Inspector General
JBAB Building 410/Door 123
250 Murray Lane, SW
Washington, DC 20222

Dear Ms. Dang:

Thank you for the opportunity to respond to the draft report "Fiscal Service Needs to Strengthen Security Controls over Public-Facing Web Servers", dated July 26, 2016. Fiscal Service agrees with the seven (7) findings and eight (8) associated recommendations, and our responses are below.

Please note that these findings and our responses, like most audits around security, can contain Sensitive But Unclassified (SBU) information that should not be publically available. We request that any SBU be redacted before publication, and will be happy to work with you on that process.

Management Response to Fiscal Service Needs to Strengthen Security Controls over Public-Facing Web Servers

Finding 1: Local Administrative Accounts Were Managed Poorly

Recommendation 1: We recommend that the Commissioner of the Bureau of the Fiscal Service ensure all user accounts are regularly reviewed and removed in accordance with NIST SP 800-53 and Fiscal Service policies and procedures.

Management Response

Fiscal Service agrees with the recommendation to ensure all user accounts are regularly reviewed and removed in accordance with NIST SP 800-53 and Fiscal Service policies and procedures. Fiscal Service has removed the inactive accounts. By June 30, 2017, Fiscal Service will ensure processes are in place to regularly review and remove user accounts that are no longer required on public-facing web servers.

Finding 2: Unauthorized Software Was Present

Recommendation 2: Establish and maintain a software asset management program to ensure that only approved software is installed on public-facing web servers.

Management Response

Fiscal Service agrees with the recommendation to establish and maintain a software asset management program to ensure that only approved software is installed on public-facing web servers. Fiscal Service currently manages a software asset management program that periodically scans for software that is hosted on Fiscal Service data center assets, including public-facing websites. This program includes the identification of the application and authorized licensing for those assets. In concert with the periodic update of the Approved Product List (APL) for the bureau, any unauthorized software is identified and designated for removal from any server in the Fiscal IT infrastructure. Fiscal Service will validate the effectiveness of the software asset management program by February 28, 2017.

Recommendation 3: Remove software that is not approved from public-facing web servers.

Management Response

Fiscal Service agrees with the recommendation and will remove any unauthorized software as described in our management response under Recommendation 2.

Finding 3: Configuration Scans Used Unapproved Baselines

Recommendation 4: We recommend that the Commissioner of the Bureau of the Fiscal Service establish a centralized process for submission, review, approval, storage, and management of security baselines and deviations that is consistent with the EITI SSP.

Management Response

Fiscal Service agrees with the recommendation to establish a centralized process for submission, review, approval, storage, and management of security baselines and deviations that is consistent with the EITI SSP. The Bureau has archived outdated files and created a new document set which contains current baselines and submission dates. These dates will be used to monitor the files and notify appropriate personnel when the document approaches its annual renewal date. Procedures for documenting baseline deviations are in draft form and will be implemented by January 31, 2017.

Finding 4: Operating Systems Were Obsolete

Recommendation 5: We recommend that the Commissioner of the Bureau of the Fiscal Service ensure that public-facing web servers are running supported operating systems so that updates are timely applied.

Management Response

Fiscal Service agrees with the recommendation to ensure that public-facing web servers are running supported operating systems so that updates are timely applied. Fiscal Service recognizes the importance of hosting services on supported operating systems and will complete the following actions by March 31, 2017:

- Complete the ongoing effort to upgrade any remaining obsolete systems
- Implement a process to proactively prevent the hosting of applications on obsolete/unsupported operating systems.

Finding 5: Ethicsburg Website Was Vulnerable to Cross-Site Scripting Attacks

Recommendation 6: We recommend that the Commissioner of the Bureau of the Fiscal Service remediate the cross-site scripting vulnerability in the Ethicsburg web site.

Management Response

Fiscal Service agrees with the recommendation to remediate the cross-site scripting vulnerability in the Ethicsburg web site. Ethicsburg will be modified to ensure input validation is in place to prevent cross-site scripting. Code changes, testing, and migration to production will be completed by January 31, 2017.

Finding 6: Sensitive Information Was Revealed In Error Messages

Recommendation 7: We recommend that the Commissioner of the Bureau of the Fiscal Service ensure that public-facing web servers used by the Administrative Resource Center website are configured to prevent disclosure of sensitive system information.

Management Response

Fiscal Service agrees with the recommendation and has taken appropriate actions to replace error messages on the ARC public-facing web servers. By January 31, 2017, Fiscal Service will validate that any default ARC error messages generated by the hosted web service that revealed sensitive information has been remediated.

Finding 7: Security Procedures Were Not Documented

Recommendation 8: We recommend that the Commissioner of the Bureau of the Fiscal Service ensure that information security procedures for public-facing servers are documented.

Appendix 2
Management Response

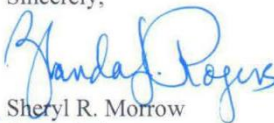
Management Response

Fiscal Service agrees with the recommendation to ensure that information security procedures for public-facing servers are documented.


To address the issue of NIST 800-53 documentation requirements, Fiscal Service has redesigned and updated document storage procedures. Fiscal Service has implemented a new program, the "CIO Publications Library", to maintain IT (including security) related procedures. This Library uses standardized document templates which include document purpose, background, related documents, scope of the document, and roles and duties assigned to personnel by the document. Management commitment is documented by requiring explicit managerial approval prior to publication of documents. Conversion of documents from the legacy IT Standards Program was completed on July 1, 2016.

Procedures related to the secure configuration and management of Fiscal Service public-facing web servers will be reviewed, and updated or developed as needed by June 30, 2017.

Sincerely,



Sheryl R. Morrow
Commissioner



Cyber/Information Technology (IT) Audit

Larissa Klimpel, Acting Director
Tram J. Dang, Director
Dan Jensen, Audit Manager
Jason Beckwith, Auditor-in-Charge
Mitul "Mike" Patel, IT Specialist
Robert Kohn, IT Specialist
James Shepard, Referencer

The Department of the Treasury

Deputy Secretary

Fiscal Assistant Secretary

Deputy Assistant Secretary Information Systems and
Chief Information Officer

Office of Strategic Planning and Performance
Improvement

Office of Deputy Chief Financial Officer, Risk and Control
Group

Bureau of the Fiscal Service

Commissioner

Chief Internal Control Officer

Office of Management and Budget

OIG Budget Examiner



Treasury OIG Website

Access Treasury OIG reports and other information online:

<http://www.treasury.gov/about/organizational-structure/ig/Pages/default.aspx>

Report Waste, Fraud, and Abuse

OIG Hotline for Treasury Programs and Operations – Call toll free: 1-800-359-3898

Gulf Coast Restoration Hotline – Call toll free: 1-855-584.GULF (4853)

Email: Hotline@oig.treas.gov

Submit a complaint using our online form:

<https://www.treasury.gov/about/organizational-structure/ig/Pages/OigOnlineHotlineForm.aspx>