



# Audit Report



OIG-12-078

INFORMATION TECHNOLOGY: Sufficient Protections Were In Place for Departmental Offices' Network and Systems

September 14, 2012

This report has been reissued to correct the report number from OIG-12-073 to OIG-12-078.

Office of  
Inspector General  
Department of the Treasury



# Contents

---

## Audit Report

Results in Brief .....	1
Background .....	2
Findings and Recommendations .....	3
Some DO LAN Devices Were Configured with Insecure Default Usernames and Passwords .....	3
Recommendation .....	4
Some DO LAN Servers Were Missing the Latest Service Packs or Running Obsolete Operating System.....	5
Recommendations.....	6
Weaknesses Were Found in Physical Security Practices at DO Buildings .....	6

## Appendices

Appendix 1: Objectives, Scope, and Methodology .....	9
Appendix 2: Management Response .....	10
Appendix 3: Major Contributors to This Report.....	13
Appendix 4: Report Distribution.....	14

## Abbreviations

DO	Departmental Offices
CIO	Chief Information Officer
LAN	Local Area Network
SP	Service Pack
UPS	Uninterruptable power supply
IT	Information Technology

**This Page Intentionally Left Blank**

---

*The Department of the Treasury  
Office of Inspector General*

September 14, 2012

Robyn East  
Deputy Assistant Secretary for Information Systems and  
Chief Information Officer

This report represents the result of our audit of network and systems security at the Departmental Offices (DO). Our overall objective was to determine whether sufficient protections existed to prevent intrusions into DO's network and systems. Specifically, we performed vulnerability assessments and penetration tests of DO's local area network (LAN), as necessarily limited by DO's operational needs and sensitivity of DO LAN's critical mission.

To accomplish our objective, we performed a series of internal vulnerability assessments and attempted penetration tests on selected DO LAN desktops, servers, equipment, and infrastructure devices. We also tested the physical security of Treasury facilities, performed social engineering testing by email phishing,<sup>1</sup> and conducted remote access security testing. In accordance with the agreed upon Rules of Engagement with the Department, we excluded a number of systems on the DO LAN and test procedures that could have adversely affected operations and resulted in denial of service attacks.

We performed our fieldwork in Washington, DC, from December 2011 through April 2012. The audit was performed in accordance with generally accepted government auditing standards. Our objectives, scope, and methodology are described in more detail in appendix 1.

## Results in Brief

We determined that DO had sufficient protections in place for its LAN. We did not find any critical vulnerabilities on the

---

<sup>1</sup> Phishing is an e-mail fraud method in which the perpetrator sends out legitimate-looking e-mail in an attempt to gather information from recipients.

---

desktops and servers tested. In addition, DO's email systems prevented our email phishing attacks from being executed successfully. However, we did identify weaknesses that should be remediated to strengthen the security protection for DO LAN. Specifically, we found some DO LAN devices were configured with insecure default usernames and passwords. We also noted a number of DO LAN servers were missing the latest service packs or running obsolete operating systems. Lastly, we identified weaknesses in physical security practices at Treasury buildings, which were quickly addressed after being identified.

We are making three recommendations to the Deputy Assistant Secretary for Information Systems and Chief Information Officer (CIO) to address these findings. With regard to the weaknesses in physical security practices, we are not making any specific recommendations at this time because after bringing it to management's attention, the matter was promptly addressed and adequately resolved during the course of our audit.

In a written response to a draft copy of this report, the Treasury CIO agreed with our findings and recommendations and provided corrective action plans (see appendix 2). Treasury's planned and reported corrective actions are responsive to the intent of our recommendations.

## **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.

---

The Department of the Treasury is organized into two major components: DO and the operating bureaus. DO is primarily responsible for the formulation of policy and management of the Department of the Treasury as a whole, while the operating bureaus and offices carry out the specific operations assigned to Treasury.

## Findings and Recommendations

### Finding 1      **Some DO LAN Devices Were Configured with Insecure Default Usernames and Passwords**

As part of our network and system security assessment of the DO LAN, we performed network scans to determine the types, names, Internet Protocol addresses,<sup>2</sup> and potential vulnerabilities of systems to test. Using the information gathered from our scans, we found that two printers, one uninterruptible power supply (UPS), and a tape backup device were configured with manufacturer preset default usernames and passwords.

Using the manufacturer preset default usernames and passwords, we were able to successfully gain administrative privileges to these devices. On both printers, we gained administrative privileges by connecting to their web interface without providing any username or password, also known as an anonymous login. We also gained administrative privileges to a UPS device and tape backup device by connecting to their web interface using the default usernames and passwords.

DO LAN System Security Plan, v1.4, dated June 29, 2011, states that DO has implemented Authenticator Management (Identification and Authentication Control). Furthermore, according to National Institute of Standards and Technology Special Publication 800-53, Revision 3, "Recommended Security Controls for Federal Information Systems," requires organizations to manage information system authenticators for

---

<sup>2</sup> An Internet Protocol address is a unique number that every device connected to the network or Internet is assigned.

---

users and devices by changing default content of authenticators upon installation.

By leaving the default usernames and passwords unchanged, anyone with internal network access could gain unauthorized access to printers and potentially use them as a platform to launch attacks against other systems connected to the DO LAN, install malicious firmware<sup>3</sup> on the printer, access any document sent to the printers, and flood the printers with print jobs. Similarly, an attacker could login to cause damage and/or loss of power to the UPS and any systems attached to it, causing potential loss of data. If a system attached to the UPS is in the middle of writing data when the attacker cut the power, the system may not be able to gracefully shutdown, and the data being written may be lost and/or corrupted. In addition, the attacker could alter the power settings on the UPS causing the device to suffer damage including, but not limited to, sparks, smoke, and fire. Lastly, using these default logins, unauthorized users could compromise tape backup devices, including changing the tape backup schedule, moving loaded tapes to unexpected locations, causing data to be overwritten, or installing malicious firmware.

Based on our Rules of Engagement, we did not attempt to perform the above actions to avoid adverse impact such as interruption of services or shutdown of these devices.

### **Recommendation**

We recommend that the CIO ensure that default user names and passwords on all devices be changed and anonymous login be disabled.

### **Management Response**

Treasury concurred with this recommendation. Treasury stated that the identified devices have been addressed to ensure that any default user name or password has been changed. Treasury

---

<sup>3</sup> Firmware is a software program or set of instructions programmed on a hardware device. It provides the necessary instructions for how the device communicates with the other computer hardware.



---

will update its procedures for installing peripheral equipment to ensure that no default user names or passwords are left on peripheral devices during the installation process. In addition, Treasury will also conduct a complete review of existing peripheral equipment to ensure that all web enabled devices have had manufacturer presets disabled. A corrective action plan will be developed and implemented by September 28, 2012.

**OIG Comment**

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

**Finding 2**

**Some DO LAN Servers Were Missing the Latest Service Packs or Running Obsolete Operating System**

From our scans, we found some servers on DO LAN were missing the most up-to-date service packs (SP) or were running obsolete operating system software. Specifically, we found:

- 15 servers were running Windows 2008 R2, SP 0. The current version is SP 1, released on February 22, 2011.
- 4 servers were running Windows 2008, SP 1. The current version is SP 2, released on April 29, 2009.
- 2 servers were running Windows 2000. This operating system is no longer supported by Microsoft as of July 13, 2010.

National Institute of Standards and Technology Special Publication 800-53, Revision 3, requires that the organization to promptly install security-relevant software updates (e.g., patches, service packs, and hot fixes).

Servers without the latest service packs may not have the most recent patches necessary to fix known software vulnerabilities, while servers running unsupported operating systems do not receive any official patches at all. As a result, the vulnerabilities from these missing patches may leave DO servers susceptible

---

to internal or external attacks which could lead to unauthorized access or compromise of Treasury's sensitive data.

**Recommendations**

We recommend that the CIO do the following:

1. Test and install the latest service packs for all servers, as appropriate.

**Management Response**

Treasury concurred with this recommendation. Treasury stated that, as of August 31, 2012, the identified systems have had the latest service packs installed.

**OIG Comment**

Management's reported corrective action is responsive to our recommendation.

2. Upgrade servers running obsolete operating systems to a supported version.

**Management Response**

Treasury concurred with this recommendation. Treasury will retire or upgrade all servers running on old operating systems. It is anticipated that this corrective action will be implemented by March 30, 2013.

**OIG Comment**

Management's planned corrective action is responsive to our recommendation.

**Finding 3**

**Weaknesses Were Found in Physical Security Practices at DO Buildings**

We found weaknesses in the physical security practices at a DO facility that allowed us unauthorized access into Treasury buildings. Specifically, we were able to bypass security

---

procedures on two occasions. An incident occurred at a DO building where we gained entry without being challenged by the officer on post. Another incident occurred where we found no officer at the entrance. Although we possess valid credentials, we were able to gain entry into the building without using the credentials. The Office of Security Programs was notified about this issue, and it was resolved promptly. Subsequently, on several occasions, we retested DO LAN physical security controls and found that the deficiencies had been addressed. Therefore, we are not making a recommendation at this time.

The DO LAN System Security Plan specifies the controls that should be in place for physical security. Such controls may include the use of guards, identification badges, or entry devices such as key cards or biometrics. According to this policy, employees entering into Treasury facilities are required to display their Treasury badge.

DO P-910, Department of the Treasury Departmental Offices Information Technology Security Policy Handbook v2.0, dated January 1, 2012, requires controls to be in place at all times to prevent unauthorized individuals from accessing DO data and system components. Specifically, individuals must have their identification checked and submit to a reasonable inspection in accordance with Treasury Directive Publication 15-71, Treasury Security Manual, Chapter V section 1, updated June 17, 2011, before being granted access to the facility.

As previously mentioned, the matter was promptly addressed and adequately resolved. Accordingly, we are not making a recommendation at this time.

---

\* \* \* \* \*

I would like to extend my appreciation to the CIO and to the DO Information Technology (IT) 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 Farbod Fakhrai, IT Audit Manager, at (202) 927-5841. Major contributors to this report are listed in appendix 4.

/s/

Tram Jacquelyn Dang  
Audit Director

The overall objective of this audit was to determine whether sufficient protections existed to prevent intrusions into Treasury's Departmental Office (DO) network and systems. This audit was included in the *Office of Inspector General Annual Plan for 2012*.

To accomplish our objective, we performed our fieldwork in Washington, DC, from December 2011 through May 2012. We performed a series of internal vulnerability assessments and attempted penetration tests on selected DO Local Area Network (LAN) desktops, servers, equipment, and infrastructure devices. We also tested the physical security of Treasury facilities, performed social engineering testing by email phishing, and conducted remote access security testing. In accordance with the agreed upon Rules of Engagement with the Department, we excluded a number of systems on the DO LAN and test procedures that could have adversely affected operations and resulted in denial of service attacks. Our tests were performed during off-peak hours to avoid unintended disruption to the network.

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  
WASHINGTON, D.C. 20220

SEP 6 2012

**MEMORANDUM FOR TRAM J. DANG**  
**AUDIT DIRECTOR**  
**OFFICE OF INSPECTOR GENERAL**

**FROM:** Robyn East   
Deputy Assistant Secretary for Information Systems  
and Chief Information Officer

**SUBJECT:** Management Response to Draft Audit Report – “FY 2012  
Sufficient Protections Were In Place for Departmental Offices’  
Network and Systems”

Thank you for the opportunity to comment on the draft audit report entitled, “FY 2012 Sufficient Protections Were In Place for Departmental Offices’ Network and Systems.” The objective of this audit was to determine whether sufficient protections existed to prevent intrusion into Treasury’s Departmental Offices’ Network and Systems. We appreciate your acknowledgement that the Departmental Offices had sufficient protections in place for its Local Area Network. We have carefully reviewed the draft and are in agreement with all findings and recommendations. Please refer to the attachment for further details on our planned corrective actions.

We appreciate the audit recommendations as they will help improve our security posture. If you have any questions, feel free to call Scott Hill, Chief Information Security Officer for Departmental Offices at 202-622-4264.

Attachment

cc: Edward A. Roback, Associate CIO for Cyber Security and Chief Information Security Officer

### Management Response to OIG Recommendations

**Note: The Department agrees with all findings and recommendations.**

#### Response to OIG Recommendations

**(U) OIG Finding 1:** Some DO LAN Devices Were Configured with Insecure Default Usernames and Passwords

**(U) OIG Recommendation 1:** We recommend that the CIO ensure that default user names and passwords on all devices be changed and anonymous login be disabled.

**(U) Treasury Response:** Treasury agrees with this recommendation. The identified devices have been addressed to ensure that any default user name or password has been changed as of July 30, 2012. Departmental Offices will update its procedures for installing peripheral equipment to ensure that no defaults are left on peripheral devices during the installation process. Departmental Offices will also conduct a complete review of existing peripheral equipment to ensure that all web enabled devices have had manufacture presets disabled. A corrective action plan will be developed and implemented. Target completion: September 28, 2012.

**(U) Responsible Official:** Departmental Offices Information System Security Officer (ISSO) for the DO LAN:

**(U) OIG Finding 2:** Some DO LAN Servers Were Missing the Latest Service Packs or Running Obsolete Operating System.

**(U) OIG Recommendation:** We recommend that the CIO do the following:

**(U) OIG Recommendation 1:** Test and install the latest service packs for all servers, as appropriate.

**(U) Treasury Response:** Treasury agrees with this recommendation. Departmental Offices has installed the service packs on the identified systems. Completed on August 31, 2012.

**(U) Responsible Official:** Departmental Offices Information System Security Officer (ISSO) for the DO LAN:

**(U) OIG Finding 2:** Some DO LAN Servers Were Missing the Latest Service Packs or Running Obsolete Operating System.

**(U) OIG Recommendation:** We recommend that the CIO do the following:

**(U) OIG Recommendation 2:** Upgrade servers running obsolete operating systems to a supported version.

**(U) Treasury Response:** Treasury agrees with this recommendation. Departmental Offices will retire or upgrade the servers running on the older operating system. A corrective action plan has

Appendix 2  
Management Response

---

been put in place and is in progress. The ISSO is currently working with the system owners to identify the schedule to upgrade all systems. Target completion date is March 30, 2013.

**(U) Responsible Official:** Departmental Offices Information System Security Officer (ISSO) for the DO LAN.



**Office of Information Technology (IT) Audits**

Tram J. Dang, Audit Director  
Farbod Fakhrai, IT Audit Manager  
Larissa Klimpel, Auditor-in-Charge  
Kevin Mfume, IT Specialist  
Mitul Patel, IT Specialist  
Don'te Kelley, IT Specialist  
Christen Stevenson, Referencer

**Department of the Treasury**

Office of the Chief Information Officer  
Office of Security Programs  
Office of Strategic Planning and Performance Management  
Office of the Deputy Chief Financial Officer, Risk and Control  
Group

**Office of Management and Budget**

Office of Inspector General Budget Examiner