Audit Report

OIG-16-050

INFORMATION TECHNOLOGY

Vulnerabilities in Security Controls Over Mint's Systems Need to Be Addressed

July 27, 2016

Office of Inspector General

Department of the Treasury

Contents

Audit Report

Appendices

Abbreviations

CDM	Continuous Diagnostics and Monitoring
CVE	Common Vulnerabilities and Exposures
ISD	Information Security Division
Mint	United States Mint
Mint SSP	United States Mint Wide Area Network General Support System System Security Plan
NIST SP	National Institute of Standards and Technology Special Publication
OIG	Treasury Office of Inspector General
TD P	Treasury Directive Publication
TNET	Treasury Network

This Page Intentionally Left Blank

July 27, 2016

Rhett Jeppson
Principal Deputy Director
United States Mint

This report represents the results of our audit of the United States Mint's (Mint) security controls over its network and information systems. 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, 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 objective for this audit was to determine whether sufficient protections exist to prevent intrusions into the Mint's network and information systems.

To accomplish our audit objective, we performed a series of internal and external vulnerability assessments and penetration tests of the Mint's workstations, servers, network-attached peripherals, infrastructure devices, and Internet websites. We also tested the physical security of the Mint's headquarters and performed social engineering tests by e-mail and phone phishing. Appendix 1 provides more detail on our objective, scope, and methodology.

Results in Brief

Overall, we found that Mint had security controls in place to prevent and detect most of our attempts to gain unauthorized access to its network and systems. Additionally, physical security controls prevented us from gaining unauthorized access

to Mint's facilities. That said, we did find deficiencies in Mint's configuration management controls that, if resolved, could help strengthen the Mint's overall security posture. Specifically, we found that some network systems were configured with factory default usernames and passwords, some decommissioned systems were still present on the network, and there were high risk vulnerabilities present on some systems that the Mint did not detect due to the limited capabilities of its scanning tools. Overall, we are making 10 recommendations 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, or have already been addressed. 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 Mint is the sole manufacturer of legal tender coinage for the Nation and is responsible for producing circulating coinage for the conduct of trade and commerce. The mission of the Mint is to serve the American people by manufacturing and distributing circulating, precious metal, and collectible coins, national medals, and providing security over assets. The Mint is headquartered in Washington, D.C., and has production facilities in Philadelphia, Pennsylvania; West Point, New York; Denver, Colorado; and San Francisco, California. The Mint is also responsible for safeguarding the majority of the United States gold reserves at the United States Bullion Depository in Fort Knox, Kentucky.

The Mint's systems are connected with each other, other bureaus' networks, and the Internet. As such, it is important that the configurations and controls that are put into place ensure that only authorized users are granted access. Unauthorized access to the Mint's network could allow an

intruder with the opportunity to compromise the confidentiality, integrity, and availability of the Mint's sensitive information. Once inside, unauthorized users could extract, delete, or modify sensitive data; discover user names and passwords; and launch denial-of-service attacks. If these unauthorized activities are not prevented or timely detected, such activities could result in compromises of information and systems, and thus hinder the Mint's mission.

Results of Audit

Finding 1 Some Network Systems Were Configured with Default Usernames and Passwords

The Mint did not ensure that factory default usernames and passwords were changed prior to deploying 14 network systems. As a result, we gained administrative access to those systems by using factory default usernames and passwords. In a few instances, the factory default was no username and password at all. Specifically, we accessed 10 multifunction printers through their web interface and were able to use one of them to send out what looked like legitimate e-mails from the Mint's helpdesk to both internal and external e-mail accounts. Additionally, we gained access to 4 network systems (i.e., a tape drive management system, an uninterruptable power supply, a data center monitoring system, and a storage system management system).

Default passwords for network systems are required to be changed upon installation in accordance with the National Institute of Standards and Technology Special Publication (NIST SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Systems and Organizations*, dated April 2013, and Treasury Directive Publication (TD P) 85-01, *Treasury Information Technology Security Program Volume 1,* dated November 2006, and the *United States Mint Wide Area Network General Support System– System Security Plan* (Mint SSP) version 9.3, dated February 6, 2014.

While the Mint SSP requires default username and password changes, the Information Security Engineer, within the Mint's

Information Security Division (ISD), stated that the Mint did not have a procedure in place to disable and/or change default administrative passwords on network systems. When the Mint's contractors installed these systems, they were unaware of requirements to change default usernames and passwords. In addition, vulnerability scans conducted by ISD in support of security authorizations and continuous monitoring did not identify this vulnerability.

By leaving accounts with factory default usernames and passwords unchanged, anyone with internal network access could gain unauthorized administrative access to these systems. This provides an opportunity for attackers to install malicious firmware, access documents sent to or copied on a multifunction printer, or use a multifunction printer as a platform to launch attacks against the Mint's network. In the case of the multifunction printer from which we sent Mint helpdesk e-mails, we could have launched social engineering attacks against Mint personnel and third-parties. Furthermore, leaving default usernames and passwords on network systems could allow attackers to compromise data, cause unexpected hazards, and destroy data and/or equipment.

Recommendations

We recommend that the Principal Deputy Director of the Mint do the following:

1. Ensure factory default user names and passwords are changed for all current systems.

   Management Response

   Management agreed with our recommendation and reported that Mint staff immediately worked to change and verify all identified default usernames and passwords when notified by the OIG. Additionally, Mint staff reviewed device configurations, identifying, and remediating any default passwords identified. Mint reported that this action was completed on July 14, 2015.

OIG Comment

Management's stated corrective actions meets the intent of our recommendation.

2. Ensure Mint develops and implements procedures to change default user names and passwords for all systems prior to deployment.

Management Response

Management agreed with our recommendation and reported that effective June 10, 2016, the Mint's procedures have been updated to change default user names and passwords for all systems prior to deployment.

OIG Comment

Management's stated corrected actions meets the intent of our recommendation.

3. Ensure that e-mails sent by network devices are clearly marked as originating from the device from which they are sent.

Management Response

Management agreed with our recommendation and responded that standard Mint configuration dictates that e-mails from network devices indicate which device is sending them. The printer identified by the OIG had been misconfigured, and the malfunction was corrected as of July 14, 2015.

OIG Comment

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

Finding 2 Some Decommissioned Systems Were Present on the Network

Mint ISD personnel were unaware that five decommissioned systems were still connected to the network. While verifying network scan results, we found that these systems were missing up-to-date patches and/or were running obsolete software. As a result, we were able to gain local administrator access to an unpatched server. When we inquired about the systems' lack of updates, Mint management realized that the systems were decommissioned and should have been removed from the network. Furthermore, management was unable to provide us with documentation to support decommissioning of the systems.

When a Federal information system is removed from operation, there are a number of risk management actions required by NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, dated February 2010. Specifically, organizations are required to update their organizational tracking and management systems (including inventory systems) to indicate the specific system components that are being removed from service; change security status reports to reflect the new status of the system; notify users and application owners hosted on the decommissioned system as appropriate; and review and assess any security control inheritance relationships for impact.

The ISD's Information Security Engineer acknowledged that policies and procedures addressing the disabling and decommissioning of systems did not exist, and the Mint's change control process did not fully ensure decommissioned systems were removed and documented. He also informed us that turnover in personnel has led to inconsistent inventory information. Additionally, he noted that Mint was unaware of the decommissioned system we were able to access because Mint's scanning tool was not configured to look for every system on the section of the network where the decommissioned system resided.

Improperly decommissioned systems still connected to the network may not be monitored and maintained. As a consequence, these systems could provide an attacker with opportunities to gain a persistent foothold to launch attacks against the network.

Recommendations

We recommend that the Principal Deputy Director do the following:

4. Establish policies and procedures to address the complete decommissioning of systems.

   Management Response

   Management agreed with our recommendation and reported that as of June 10, 2016, the Mint has developed policies and procedures to address the complete decommissioning of systems.

   OIG Comment

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

5. Ensure all systems slated for decommissioning are documented and decommissioned.

   Management Response

   Management agreed with our recommendation and reported that as of June 10, 2016, the Mint has implemented measures to ensure all systems slated for decommissioning are documented and decommissioned.

   OIG Comment

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

6. Ensure scanning capabilities look for all connected systems and scan results are reconciled against the Mint's inventory.

Management Response

Management agreed with our recommendation and responded that the Mint continues to improve its vulnerability scanning program by regularly reviewing scan policies and scanned ranges. In addition, the Mint is actively engaged with Treasury, DHS [Department of Homeland Security], and the contract integrator to deploy Phase 1 of Continuous Diagnostics and Monitoring (CDM) which will cover Hardware Asset Management, Software Asset Management, Vulnerability Management, Configuration Management, and scan all inventoried systems at least every 72 hours. The current target date for full operational capability of the CDM tools and dashboard at the Mint is October 1, 2017.

OIG Comment

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

Finding 3 High Risk Vulnerabilities Were Present on Mint's Systems

We identified and confirmed 82 unique high-risk vulnerabilities present on the Mint's systems.[1] Of this total, 34 unique vulnerabilities related to obsolete versions of Oracle or VMWare, which could have been remediated by updating to the latest version of the software; another 26 unique vulnerabilities related to unpatched software, system services, or protocols; and 22 unique vulnerabilities related to insecurely configured software that could be remediated by changing the

[1] High risk is defined as those vulnerabilities ranked by Nexpose as critical and severe, which pose a potential threat.

configuration settings. These 82 vulnerabilities are among the common vulnerabilities and exposures described on the Common Vulnerabilities and Exposures (CVE®) website. CVE is a dictionary of common names (i.e., CVE Identifiers) for publicly known cybersecurity vulnerabilities and is available for public use.[2]

According to NIST SP 800-53, Revision 4, an organization should employ vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned. Additionally, the Mint SSP requires that scanning tools are automatically updated with current threats and vulnerabilities, and that a variety of vulnerability scanning tools are deployed for system and application vulnerability identification and remediation.

The ISD staff informed us that the Mint's vulnerability scanner did not have the capability to detect the vulnerabilities that we identified. Management further stated that it has not been able to address the scanner issue due to limited number of staff.

If high-risk vulnerabilities are present on a network, attackers could exploit them in order to gain unauthorized access to network resources, personally identifiable information, proprietary information, and intellectual property. Furthermore, vulnerabilities that are listed in the CVE contain technical details that attackers could exploit. If a vulnerability scanner fails to detect published vulnerabilities, management could have a false sense of security and not take the actions necessary to address the risks that might be present.

[2] CVE® (https://cve.mitre.org)

Recommendations

We recommend that the Principal Deputy Director do the following:

7. Ensure that obsolete software is either removed or upgraded.

   Management Response

   Management agreed with our recommendation and noted that the implementation of Phase I of CDM will address this recommendation by October 1, 2017.

   OIG Comment

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

8. Ensure software patches and updates are timely applied.

   Management Response

   Management agreed with this recommendation and noted that the Implementation of Phase I of CDM will address this recommendation by October 1, 2017.

   OIG Comment

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

9. Ensure systems and software are securely configured.

   Management Response

   Management agreed with this recommendation and noted that the implementation of Phase I of CDM will address this recommendation by October 1, 2017.

OIG Comment

Management's planned correction action meets the intent of our recommendation.

10. Ensure scanning capabilities detect published vulnerabilities.

Management Response

Management agreed with this recommendation and noted that the implementation of Phase 1 of CDM will address this recommendation by October 1, 2017.

OIG Comment

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

* * * * * *

I would like to extend my appreciation to the Principal Deputy Director of the Mint 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 Larissa Klimpel, Audit Manager, at (202) 927-0361. Major contributors to this report are listed in appendix 3.

/s/

Tram Jacquelyn Dang
Director, Information Technology Audit

To support our ongoing oversight of the *Federal Information Security Modernization Act of 2014,* we perform periodic audits of networks and information security of Department of the Treasury (Treasury) bureaus and offices. Our objective for this audit was to determine whether sufficient protections exist to prevent intrusions into the United States Mint's (Mint) network and information systems.

To accomplish our objective, we performed a series of internal and external vulnerability assessments and penetration tests on the Mint's workstations, servers, network-attached peripherals (such as cameras and printers), infrastructure devices, and Internet websites. Specifically, we performed an internal assessment of the Mint's network, behind Treasury Network (TNet[3]) firewalls, with full knowledge of the Mint. We were provided the same system access, physical assets, information, and other resources available to the Mint's employees stationed at Mint headquarters. We also used Office of Inspector General (OIG) owned and licensed hardware and software, including Core Impact and Nexpose.

During our tests, we notified the Mint's information security management and staff of issues we discovered that we believed may have been indicative of serious problems that would require their immediate attention. While at Mint headquarters, we performed social engineering tests by e-mail and phone phishing to determine whether the Mint's help desk was able to prevent and detect attempts at impersonating Mint employees.

We performed our external assessments from OIG headquarters via an Internet Service Provider connections, using OIG's hardware and software and information available to the general public. We performed our audit work at Mint headquarters in Washington, D.C., between February and September 2015.

[3] TNet is a wide area network that provides Treasury with e-mail, Internet, and voice traffic applications.

We conducted our 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.

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

FROM: Rhett Jeppson /s/
Principal Deputy Director
United States Mint

SUBJECT: Management Response to Draft Audit Report, "Vulnerabilities in Security Controls over Mint's Systems Need to be Addressed"

The United States Mint appreciates the opportunity to comment on the draft report entitled, "Vulnerabilities in Security Controls over Mint's Systems Need to be Addressed." The objective of the audit was to determine if the United States Mint had security controls in place to prevent and detect unauthorized access to its network and systems, as well as physical controls to prevent unauthorized access to United States Mint facilities. As noted in the report, overall the audit deemed that the United States Mint had security controls in place to prevent and detect most attempts executed during the audit for access to the United States Mint network, systems, and facilities.

We have reviewed the draft report and are in agreement with all of the findings as outlined. Upon notification of the vulnerabilities outlined in the draft report, the United States Mint began the process of remediating the vulnerabilities identified. Some of the recommendations addressed in the report have been completed for which you will find the action taken and date of closure in our attached response. For recommendations that have not been closed, we have provided corrective actions with corresponding due dates for closure. All responses can be found in the attached document entitled, "Appendix A - United States Mint, Management Response to OIG recommendations."

Again, we appreciate the audit recommendations that will assist the United States Mint to improve our security posture. If you have any questions, please contact Ray Hardy, Chief Information Security Office for the United States Mint, at 202-354-7569.

Attachment

Appendix A

United States Mint Management Response to OIG recommendations

Finding 1: Some Network Systems Were Configured with Default Usernames and Passwords

Recommendation 1: Ensure factory default user names and passwords are changed for all current systems.

Mint Response: The United States Mint (Mint) agrees with this recommendation. When notified by the OIG, Mint staff immediately worked to change and verify all identified default usernames and passwords. Additionally, Mint staff reviewed device configurations, identifying and remediating any default passwords identified. This action was completed on July 14, 2015.

Responsible Official: Acting Branch Chief Data Center & Data Network

Recommendation 2: Ensure the Mint develops and implements procedures to change default user names and passwords for all systems prior to deployment.

Mint Response: The Mint agrees with this recommendation. In accordance with TDP-85-01, effective June 10, 2016, Mint procedures have been updated to change default user names and passwords for all systems prior to deployment.

Responsible Official: Acting Branch Chief Data Center & Data Network

Recommendation 3: Ensure that e-mails sent by network devices are clearly marked as originating from the device from which they are sent.

Mint Response: The Mint agrees with this recommendation. Standard Mint configuration dictates that e-mails from network devices indicate which device is sending them. The printer identified by the OIG had been misconfigured, and the malfunction has been corrected as of July 14, 2015.

Responsible Official: Acting Branch Chief Data Center & Data Network

Finding 2: Some Decommissioned Systems Were Present on the Network

Recommendation 4: Establish policies and procedures to address the complete decommissioning of systems.

Mint Response: The Mint agrees with this recommendation. As of June 10, 2016, the Mint has developed policies and procedures to address the complete decommissioning of systems.

Responsible Official: Chief Information Security Officer

Recommendation 5: Ensure all systems slated for decommissioning are documented and decommissioned.

Mint Response: The Mint agrees with this recommendation and has implemented the measures as indicated in the response to Recommendation 4 to ensure that all systems slated for decommissioning are documented and decommissioned. This was completed June 10, 2016.

Responsible Official: Chief Information Security Officer

1

Recommendation 6: Ensure scanning capabilities look for all connected systems and scan results are reconciled against the Mint's inventory.

Mint Response: The Mint agrees with this recommendation. The Mint continues to improve its vulnerability scanning program by regularly reviewing scan policies and scanned ranges. The Mint is actively engaged with Treasury, DHS, and the contract integrator to deploy Phase 1 of Continuous Diagnostics and Monitoring (CDM), which will cover Hardware Asset Management, Software Asset Management, Vulnerability Management, and Configuration Management. This will ensure positive control over all inventoried systems, and that all systems in inventory are scanned at least every 72 hours. The current target date for Full Operational Capability (FOC) of the CDM tools and Dashboard at the Mint is October 1, 2017.

Responsible Official: Chief Information Security Officer

Finding 3: High-Risk Vulnerabilities Were Present on Mint's Systems

Recommendation 7: Ensure that obsolete software is either removed or upgraded.

Mint Response: The Mint agrees with this recommendation. The implementation of Phase I of CDM, as noted in Recommendation 6, will address this by ensuring that obsolete software is either removed or upgraded. This will be completed by October 1, 2017.

Responsible Officials: Acting Branch Chief Data Center and Data Network and Chief Information Security Officer

Recommendation 8: Ensure software patches and updates are timely applied.

Mint Response: The Mint agrees with this recommendation. The Implementation of Phase I of CDM, as noted in Recommendation 6, will address this by ensuring that software patches and updates are timely applied. This will be completed by October 1, 2017.

Responsible Officials: Acting Branch Chief Data Center & Data Network and Chief Information Security Officer

Recommendation 9: Ensure systems and software are securely configured.

Mint Response: The Mint agrees with this recommendation. The implementation of Phase I of CDM, as noted in Recommendation 6, will address this by ensuring that systems and software are securely configured. This will be completed by October 1, 2017.

Responsible Officials: Acting Branch Chief Data Center & Data Network and Chief Information Security Officer

Recommendation 10: Ensure scanning capabilities detect published vulnerabilities.

Mint Response: The Mint agrees with this recommendation. The implementation of Phase 1 of CDM, as noted in Recommendation 6, will address this by ensuring that scanning capabilities detect published vulnerabilities. This will be completed by October 1, 2017.

Responsible Official: Chief Information Security Officer

Office of Information Technology Audits

Tram J. Dang, Information Technology Audit Director
Larissa Klimpel, Information Technology Audit Manager
Don'te Kelley, Auditor-in-Charge
Jason Beckwith, Information Technology Specialist
Mitul "Mike" Patel, Information Technology Specialist
Patrick Arnold, Referencer

The Department of the Treasury

Deputy Secretary
Deputy Assistant Secretary Information Systems and Chief Information Officer
Office of Strategic Planning and Performance Management
Risk and Control Group, Office of Deputy Chief Financial Officer

United States Mint

Principal Deputy Director, United States Mint

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