



OFFICE *of*
INSPECTOR GENERAL
★ ★ ★ ★
UNITED STATES DEPARTMENT OF
HOUSING AND URBAN DEVELOPMENT

Assessment of HUD's IT Infrastructure To Support Extensive Telework

HUD's IT Infrastructure Needs Improvement |

2023-FO-0008

January 24, 2023

Date: January 24, 2023

To: Beth Niblock
Chief Information Officer, Q

From: Kilah S. White
Assistant Inspector General for Audit, GA

Subject: HUD's IT Infrastructure Needs Improvement

Attached are the U.S. Department of Housing and Urban Development (HUD), Office of Inspector General's (OIG) final results of our review of HUD's information technology (IT) infrastructure to support extensive mandatory telework during the COVID-19 pandemic.

HUD Handbook 2000.06, REV-4, sets specific timeframes for management decisions on recommended corrective actions. For each recommendation without a management decision, please respond and provide status reports in accordance with the HUD Handbook. Please furnish us copies of any correspondence or directives issued because of the audit.

The Inspector General Act, Title 5 United States Code, appendix 8M, requires that OIG post its reports on the OIG website. Accordingly, this report will be posted at <https://www.hudoig.gov>.

If you have any questions or comments about this report, please do not hesitate to call Brittany Wing, Audit Director, at (202) 302-7296.

Highlights

HUD'S IT INFRASTRUCTURE NEEDS IMPROVEMENT | 2023-FO-0008

What We Audited and Why

We audited the U.S. Department of Housing and Urban Development's (HUD) information technology (IT) infrastructure to support mandatory telework. During mandatory telework, more employees simultaneously needed remote access to HUD's network and agency resources for an extended period, which presented unique risks and security requirements. The objective of our audit was to assess HUD's IT infrastructure preparedness and capability to support extensive mandatory telework during the COVID-19 pandemic. While HUD is no longer operating under mandatory telework, understanding the challenges it faced is key to managing a flexible workforce and preparing for future emergencies.

What We Found

HUD experienced challenges with its IT infrastructure while under mandatory telework. We found (1) there were significant delays in processing computer security updates, (2) users encountered months of network performance issues, (3) the user password expiration policy was not enforced, and (4) the help desk system did not capture complete data. These conditions occurred because HUD's virtual private network (VPN) bandwidth was not sufficient to accommodate the significant increase in users' simultaneously needing remote access and because there were limitations in the technical environment and weaknesses in the help desk system's controls. As a result, (1) HUD was vulnerable to cyber-attacks and unauthorized access, (2) HUD's ability to accomplish its mission could be affected, and (3) HUD did not have assurance that all IT problems reported by users were resolved. Although HUD experienced challenges during mandatory telework, HUD continued its operations; increased network capacity; and plans to make additional network improvements, resume password policy enforcement, and potentially replace its help desk system. HUD needs to fully address the underlying causes of the issues identified so that it can manage its flexible workforce in a way that minimizes risk and prepares it for future emergencies.

What We Recommend

We recommend that HUD's Office of the Chief Information Officer research, evaluate, and implement technical or alternative solutions to (1) deploy essential computer software updates using secure methods to ensure that computer security updates occur in a timely manner to minimize risk to HUD's systems and operations; (2) provide additional improvements to VPN-related remote working capabilities, including performing routine VPN stress tests as part of its contingency planning and testing processes; (3) resolve user account management issues; and (4) assess its help desk system against other technical solutions and ensure that the help desk solution used captures complete data on technical support requests. These measures include but are not limited to ensuring that sequence gaps are properly documented or do not occur, valid transactions are accepted by the help desk system, rejected transactions are identified, and the history of each transaction is retained.

Table of Contents

Background and Objective	5
Results of Audit.....	6
Finding 1: HUD Experienced Difficulties and Significant Delays in Processing Computer Security Updates.....	6
Finding 2: HUD System Users Encountered Network Performance Issues.....	9
Finding 3: HUD Has Not Enforced Its User Password Expiration Policy	11
Finding 4: HUD Has Weaknesses in Controls Over Its National Help Desk System	14
Scope and Methodology	16
Appendixes	17
APPENDIX A - AUDITEE COMMENTS AND OIG’S EVALUATION.....	17

Background and Objective

The U.S. Department of Housing and Urban Development's (HUD) mission is to create strong, sustainable, inclusive communities and quality affordable homes for all. It accomplishes this mission through a variety of programs administered by more than 7,000 employees. The mission of its Office of the Chief Information Officer (OCIO) is to enable delivery of HUD programs, services, and management processes by providing high-quality information, technology solutions, and services.

HUD encourages and supports the use of telework to enhance its work and the work and life of its employees. Telework provides benefits in several areas, such as (1) recruiting and retaining the best possible workforce; (2) helping employees manage long commutes and other work-life issues; (3) reducing traffic congestion, emissions, and infrastructure impact in urban areas; and (4) ensuring continuity of essential functions in the event of national or local emergencies.

On March 20, 2020, HUD employees entered an unprecedented mandatory telework environment during the coronavirus disease of 2019 (COVID-19) pandemic. This event followed a series of Office of Management and Budget (OMB) memorandums¹ to Federal agencies addressing increased telework during the pandemic. On March 27, 2020, Congress passed the Coronavirus Aid, Relief, and Economic Security (CARES) Act. The CARES Act provided HUD with approximately \$12 billion to mitigate the effects of the COVID-19 crisis and the ability to waive certain requirements. Of that amount, \$35 million was appropriated for HUD's administrative support offices to be used for salaries and expenses, information technology (IT) purposes, and to support telework.

Before the pandemic, HUD reported² that 20 percent of its employees participated in regular telework 3 or more days per week, 26 percent participated in regular telework 1-2 days per week, and 36 percent participated in situational telework. During mandatory telework, more employees simultaneously needed remote access to HUD's network and agency resources for an extended period, which presented unique risks and security requirements.

HUD uses a national help desk to provide employees and other HUD system users with a customer-focused, single-point-of-contact technical support service for answering calls and providing personal customer assistance. The HUD national help desk receives calls 24 hours a day, 7 days a week. Customers can call the national help desk any time and get assistance from a national help desk analyst. The HUD national help desk provides resolution and escalation services for IT problems encountered while working, including workstation computer problems and password resets.

¹ OMB Memorandums M-20-13 encouraged agencies to use of telework flexibilities, M-20-15 provided updated guidance for the National Capital Region, and M-20-16 required agencies to maximize telework across the Federal workforce, including mandatory telework if necessary, while maintaining mission-critical needs.

² OMB Fiscal Year 2019 Status of Telework in the Federal Government Report to Congress, page 90

Results of Audit

FINDING 1: HUD EXPERIENCED DIFFICULTIES AND SIGNIFICANT DELAYS IN PROCESSING COMPUTER SECURITY UPDATES

HUD was unable to process timely security updates while under mandatory telework. To complete security updates on users' computers, a functioning technical approach is necessary to deploy the updates and monitor their implementation. In this case, more than two-thirds of HUD's laptop and desktop computers did not receive key security updates for more than 200 days. This condition occurred because HUD's virtual private network (VPN)³ bandwidth was not sufficient to accommodate the significant increase in the number of users accessing the network simultaneously during mandatory telework. As a result, HUD users were conducting business with computers that had not received the security updates, and HUD did not have reasonable assurance that cyber attackers could not find and exploit software vulnerabilities. Although HUD had made increases to network capacity that enabled it to process computer security updates for employees working remotely, additional improvements are needed to ensure that future security updates are processed in a timely manner to minimize risk to its systems and operations.

HUD Did Not Fully Process Three Software Updates for More Than 200 days

HUD was unable to fully process software updates for security vulnerabilities while under mandatory telework during the COVID-19 pandemic. It scheduled three updates to begin deployment on March 15, 2020. However, nearly 5,100 HUD computers had not received the security updates more than 200 days after the deployment notice. As a result, more than two-thirds of users' laptop and desktop computers operated without security patches during this period.

Many vendors, such as Microsoft, automatically release new patches each month to address vulnerabilities. The longer computers go without security updates, the more likely published vulnerabilities can be exploited by cyber criminals. To complete security updates on users' computers, organizations need a functioning technical approach to deploy the updates and monitor their implementation. HUD's IT policy⁴ required program offices-system owners to maintain a flaw remediation program and manage software updates for HUD mission-business applications. The policy⁵ also required OCIO to install security patches to servers and workstations promptly.

³ A virtual private network, or VPN, is an encrypted connection over the internet from a device to a network. The encrypted connection helps ensure that sensitive data are safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely.

⁴ Information Technology Security Policy, HUD Handbook 2400.25, REV-4.2, section 4.7.2 (The applicable HUD criteria used at the time assignment was initiated).

⁵ Information Technology Security Policy, HUD Handbook 2400.25, REV-4.2, section 4.7.3 (The applicable HUD criteria used at the time assignment was initiated).

In this case, for more than 200 days, more than two-thirds of HUD’s laptop and desktop computers did not receive key security updates that would have resolved vulnerabilities and resulted in quality improvements to future security updates. This condition occurred because HUD’s VPN bandwidth was not sufficient to accommodate the significant increase in the number of users accessing the network simultaneously during mandatory telework. Additionally, HUD delayed deploying the updates to its full workforce because its platform was not technically sufficient to support remote deployment of the software security updates, and unsuccessful software updates may not have been resolved until the user returned to the office.

As a result, HUD users conducted business with computers that had outdated software, and HUD did not have reasonable assurance that cyber attackers could not find and exploit vulnerabilities in commonly used software and other system weaknesses. This condition could allow cyber criminals to hack into user computers and potentially result in damages to the agency’s systems and operations. For example, an attacker who successfully exploited the .NET Framework⁶ vulnerability on computers without the update could run arbitrary code in the context of the current user. If the current user was logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The table below describes the risks that existed due to each of the delayed security updates:

Item	Knowledge Base Article ⁷	Risk of Delayed Updates
1	KB4537759	This security update would resolve vulnerabilities in the Adobe Flash Player ⁸ software that is installed on many of the Windows operating systems. ⁹ Not receiving this update in a timely manner is important because the software is widely used to for delivering high-impact, rich web content. For example, in a web-based attack scenario, the object is to convince a user to visit the website, typically by getting the user to click on a link in an email message or instant message. In addition, compromised websites and websites that accept or host user-provided content or advertisements could contain specially crafted content that could exploit these vulnerabilities.
2	KB4552152	This update would fix the reliability of the windows update process. Servicing stack updates ensure a robust and reliable windows update process, so that devices can receive and install Microsoft updates and security fixes. Not receiving servicing stack updates in a

⁶ .NET Framework is a software development framework for building and running applications on Windows

⁷ Security updates are accompanied by a bulletin that is published by Microsoft. The knowledge base article typically contains more information about an individual bulletin, including workarounds, known issues, details about downloadable files, and details about files installed or replaced as part of an update.

⁸ Adobe Flash Player is a product for delivering high-impact, rich web content.

⁹ The operating system is a master control program that runs the computer and acts as a scheduler and traffic controller. The operating system is the first program copied into the computer’s memory after the computer is turned on.

		timely manner could impede a computer’s ability to receive future security updates, making the computer vulnerable to attack.
3	KB4552931	This update would resolve a vulnerability when a user opens a specially crafted file with an affected version of .NET Framework. Not receiving this update in a timely manner could make the computer vulnerable to an email attack scenario in which an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. If the user opened the file, the attacker could take control of the system and attack the computer as described above.

HUD Had Begun To Address the Weaknesses But More Improvements are Needed

According to HUD, it began increasing network capacity to its data centers in July 2020, which enabled it to process computer security updates for HUD staff when working remotely. Although HUD’s actions improved their ability to process during remote work, the weakness has not been fully addressed and still exists. To further address the weakness, HUD planned to implement additional improvements to its ability to process computer security updates by using a direct internet solution. HUD did not provide timeframes of when these improvements would be implemented.

Conclusion

One of the best ways to protect systems is to ensure that computers have the latest security updates because cyber criminals are constantly finding and exploiting new software vulnerabilities and weaknesses. The longer computers go without security updates, the more likely published vulnerabilities can be exploited by cyber criminals. For more than 200 days, HUD was unable to fully process software updates in a timely manner, which would have (1) resolved vulnerabilities in the Adobe Flash Player, which is installed on many of the Windows operating systems; (2) resulted in quality improvements to the servicing stack, which is the component that installs Microsoft Windows updates and security fixes; and (3) addressed the remote code execution vulnerability that existed in the .NET Framework software. This condition occurred because of VPN bandwidth capacity limitations. Additionally, HUD delayed deploying the updates to its full workforce because its platform was not technically sufficient to support remote deployment of the software security updates. Although HUD had begun to address the weaknesses cited through increased network capacity to its data centers, HUD is still at risk until additional improvements are completed to ensure that future security updates are processed in a timely manner to minimize risk to its systems and operations.

Recommendations

We recommend that the Office of the Chief Information Officer

- 1A. Research, evaluate, and implement technical or alternative solutions to deploy essential computer software updates using appropriate secure methods to ensure that computer security updates occur in a timely manner to minimize risk to HUD’s systems and operations

FINDING 2: HUD SYSTEM USERS ENCOUNTERED NETWORK PERFORMANCE ISSUES

HUD system users encountered months of network performance issues during mandatory telework, such as difficulty in maintaining VPN connections, delays in sending email, an inability to access systems, and routine tasks' taking longer than normal. This condition occurred because HUD's VPN did not have the capacity¹⁰ to handle the demand of extensive mandatory telework and because HUD had not performed a VPN stress test to identify and prevent potential network issues. Network performance issues can affect HUD's ability to accomplish its mission. Although HUD had begun to address the weaknesses cited by increasing network capacity, additional improvements are needed to build a more resilient network and a process to regularly identify and remediate network performance issues.

Network Performance Issues Impacted Users

HUD system users encountered months of network performance issues during mandatory telework. Between March and June 2020 there were 5,949 help desk tickets related to VPN issues. For example, users experienced (1) difficulty in maintaining an active VPN connection for more than a few minutes at a time, (2) delays in sending emails, (3) an inability to access systems or slowness when gaining access, and (4) routine tasks' taking a longer than normal time to perform.

Information systems and networks are vulnerable to a variety of disruptions, ranging from mild to severe. While it is virtually impossible to eliminate all disruptions, they can be minimized or eliminated through management, operational, and technical controls as part of an organization's resiliency¹¹ efforts. Contingency planning mitigates these risks by providing effective and efficient solutions to enhance system availability. National Institute of Standards and Technology (NIST) Special Publication 800-53¹² recommends that the organization identify essential missions and business functions and associated contingency requirements. Additionally, HUD's IT policy¹³ requires program offices to develop contingency plans, including a business impact analysis, for information systems under their control and for high-impact systems, in which applicable system owners are required to conduct capacity planning so that the necessary capacity for information processing, telecommunications, and environmental support exists during crisis situations.

In this case, HUD's VPN did not have the capacity to handle the increased demand for remote information processing during extensive mandatory telework. OCIO acknowledged that if HUD upgraded its network in previous years, before it activated mandatory telework across the agency, the system would have had

¹⁰ Capacity of the network includes various resources required to prevent a performance or availability impact on business-critical applications.

¹¹ Resilience is the ability to quickly adapt and recover from any known or unknown changes to the environment.

¹² NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Section CP-2, Contingency Plan

¹³ Information Technology Security Policy, HUD Handbook 2400.25, REV-4.2, section 4.4.2

fewer capacity-related issues. Additionally, HUD had not performed a VPN stress test,¹⁴ which could have helped OCIO identify network issues and allowed for timely remediation to ensure that HUD was prepared to support a scenario in which all employees work remotely for an extended period.

Network performance issues could affect HUD's ability to accomplish its mission. For example, even relatively minor interruptions to processing electronically maintained information can result in inaccurate and incomplete data or have financial impacts, such as transactions' not fully processing. These performance issues occurred at a time when HUD was managing billions of dollars in grants because of COVID-19.

HUD Had Begun To Address the Weaknesses Cited But Additional Actions are Needed

According to HUD, it began to address the weaknesses cited by increasing network capacity to its data centers in July 2020, increasing the number of VPN licenses it had for each data center, and splitting users between its primary and backup data centers to reduce the load on its VPN and limit the impact of the network performance issues. The actions HUD took provided improvement during the period of remote work; however, the weakness still exists, and additional actions are needed to fully address it. HUD also planned to implement additional improvements to the VPN hardware to ensure that the agency has adequate failover capabilities and a strong continuity of operations solution. HUD did not provide timeframes when the additional improvements would be made.

Conclusion

While information systems and networks are vulnerable to a variety of disruptions, organizations should continually work to adapt to changes and risks that can impact their ability to continue critical functions. During mandatory telework, users encountered months of network performance issues due to deficiencies in HUD's VPN capacity. Although HUD had begun to address the weaknesses cited through increased network capacity, additional improvements are needed to build a more resilient network and a process to regularly identify and remediate network performance issues.

Recommendations

We recommend that the Office of the Chief Information Officer

- 2A. Research, evaluate, and implement technical solutions to provide additional improvements to VPN and related remote working capabilities of HUD system users.
- 2B. Perform routine VPN stress tests as part of its contingency planning and testing processes to regularly identify and remediate network performance issues and ensure that network capabilities are sufficient for teleworking.

¹⁴ VPN stress tests involve testing a VPN with large quantities of data and many users to evaluate its performance during peak periods.

FINDING 3: HUD HAS NOT ENFORCED ITS USER PASSWORD EXPIRATION POLICY

HUD was not able to enforce its password policy while under mandatory telework. This condition occurred due to limitations in the technical environment, which reduced HUD's ability to conduct some password controls-related procedures when users worked remotely. Because HUD did not enforce its password policy, it increased the risk of unauthorized users' accessing its systems, which potentially diminished the reliability of its computerized data and increased the risk of destruction or inappropriate disclosure of data in its systems. While HUD indicated that it planned to begin enforcing the policy again and implement an enterprise solution, it needs to show that it has fixed the underlying issue in the technical environment.

HUD's Password Policies Were Not Enforced

While under mandatory telework during the COVID-19 pandemic, HUD made a risk based decision to not enforce its password policy, including for passwords for users' computers and applications that use active directory¹⁵ passwords. However, after mandatory telework was lifted, HUD was still not enforcing the policy more than 2 years later. Instead, HUD allowed its password policy to be overridden, and passwords were set to not expire.

Account policies such as password policies should be formally established and enforced based on risk. NIST Special Publication 800-53¹⁶ recommends that organizations change authenticators for system users after a time assigned by the organization. Additionally, HUD's IT policy¹⁷ states that program offices need to ensure that information systems' access control measures are in place to provide protection from unauthorized alteration, loss, unavailability, or disclosure of information. Identification and authentication should be unique to each user or processes acting on behalf of users.¹⁸ Password controls are part of the identification and authentication mechanisms of logical access controls and typically include changing passwords periodically, about every 30 to 90 days. The more sensitive the data or function, the more frequently passwords should be changed.¹⁹

HUD's national help desk began²⁰ overriding the password expiration policy around March 17, 2020, and on March 26, 2020, HUD OCIO sent a notification to all staff members with conflicting information,

¹⁵ An active directory is a Microsoft technology used to manage computers and other devices on a network.

¹⁶ NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Section IA-5, Authenticator Management

¹⁷ Information Technology Security Policy, HUD Handbook 2400.25, REV-4.2, section 5.2.2

¹⁸ Federal Information Processing Standards Publication 200, Minimum Security Requirements for Federal Information and Information Systems, Identification and Authentication (IA), page 2, chapter 3

¹⁹ Federal Information System Controls Audit Manual (FISCAM), February 2009, Access Controls, AC-2.1, page 216

²⁰ This information is based on a review of help desk tickets created between March and June 2020. During this period, approximately one in five tickets were related to password issues.

stating in part that “regularly changing your network password is vital in safeguarding your information,” while also telling employees to “... not attempt to change your password while teleworking.” On April 16, 2020, nearly a month after HUD’s national help desk began overriding the password expiration policy, HUD OCIO documented its decision to accept risks for HUD’s user account management-related controls on the local area network and wide area network due to the COVID-19 pandemic. HUD OCIO extended this risk acceptance on May 12, 2020. As of June 2022, HUD was still not enforcing the policy.

The condition above occurred due to limitations in the technical environment during the COVID-19 pandemic, such as bandwidth and VPN issues. This drastically reduced OCIO’s ability to conduct some password controls-related procedures due to HUD users’ working remotely. For example, users who were working remotely needed to be successfully connected to the VPN to change passwords. If a user’s attempt to change a password remotely was not successful on the domain controller,²¹ the user would lose his or her domain connection, requiring him or her to report to the office to physically connect to the office network to log in.

For access controls to be effective, they should be properly authorized, implemented, and maintained. Because HUD did not enforce its password policy, it increased the risk of unauthorized users’ accessing its systems, which could potentially diminish the reliability of its computerized data and increase the risk of destruction or inappropriate disclosure of data. For example, unauthorized individuals, such as outside intruders and former employees, could secretly read and copy sensitive data and make undetected changes or deletions for malicious purposes or personal gain.

HUD Planned To Begin Enforcing Its Policy and Implement an Enterprise Solution

In June 2022, HUD stated that it planned to begin enforcing its password policy and to implement an enterprise solution to make additional access control improvements. However, additional actions are needed. Specifically, HUD needs to demonstrate that it has not only begun to enforce its password policies, but has fixed the underlying issues, such as bandwidth and VPN issues, in the technical environment.

Conclusion

Enforcement of password policies is necessary to protect the confidentiality of information and the integrity of systems by keeping unauthorized users out of systems. Without enforcement of adequate access controls, unauthorized individuals, such as outside intruders and former employees, could secretly read and copy sensitive data and make undetected changes or deletions for malicious purposes or personal gain. HUD did not enforce its password policy during the mandatory COVID-19 telework. As of June 2022, the policy was not being enforced. While HUD indicated that it planned to begin enforcing the policy again and implement an enterprise solution, it needs to show that it has fixed the underlying issue in the technical environment.

²¹ A domain controller is a server that verifies users on computer networks.

Recommendations

We recommend that the Office of the Chief Information Officer

- 3A. Research, evaluate, and implement technical solutions to resolve the user account management issues and the underlying issue in the technical environment.

FINDING 4: HUD HAS WEAKNESSES IN CONTROLS OVER ITS NATIONAL HELP DESK SYSTEM

Limited functionality within HUD's helpdesk system did not ensure that it captured complete data on technical support requests during mandatory telework. Specifically, the data contained gaps in the ticket numbers assigned to user interactions with the national help desk, which means that information may be missing for nearly 1 in 10 national help desk interactions with users. This condition occurred because of weaknesses in the system's entry and processing controls. As a result, HUD could not provide reasonable assurance that it was aware of all IT problems reported by users and that issues not captured were resolved or escalated when necessary. Although HUD stated that it was evaluating a different help desk solution, the issues identified are ongoing and could erode user confidence in HUD's national help desk system until they are resolved.

HUD's National Help Desk System Does Not Capture All Data

HUD's national help desk system did not ensure that it captured complete data on technical support requests during mandatory telework. Specifically, it contained gaps in the ticket numbers assigned to user interactions with the national help desk. The system contained data on more than 55,000 tickets created between March and June 2020, which included several months of mandatory telework. However, there were more than 5,800 missing ticket numbers in the data based on gaps in the ticket number sequencing, which means that information may be missing for nearly 1 in 10 national help desk interactions with users during this period.

HUD's national help desk receives calls related to technical support for employees and other system users 24 hours a day, 7 days a week. It is responsible for resolving and escalating problems when needed and recording data on interactions with users. Organizational procedures for information systems should reasonably ensure that (1) all data entry is done in a controlled manner; (2) data entry into the application is complete, accurate, and valid; (3) any incorrect information is identified, rejected, and corrected before processing; and (4) the confidentiality of data is adequately protected.²² HUD's IT policy²³ required that for moderate- or high-impact systems, the program offices-system owners ensure that the information system checks data entry for accuracy, completeness, and validity. Additionally, it required that system owners ensure that audit trails were sufficient in detail to facilitate the reconstruction of events if a system was compromised or if a malfunction occurred or was suspected.

This condition occurred because of weaknesses in the system's entry and processing controls. For example, HUD stated that the gaps identified could have been caused by the system's not retaining data on tickets that were started but not saved or timed out before they were saved as well as tickets that were canceled or abandoned because the user called to obtain an update about a previous ticket. HUD noted that the help desk system did not track or retain ticket data in these circumstances.

²² FISCAM, February 2000, Critical Element BP-1, page 402

²³ Information Technology Security Policy, HUD Handbook 2400.25, REV-4.2, sections 4.7.9 and 5.3.3

Without adequate entry and processing control measures, HUD cannot provide reasonable assurance that all technical support requests were entered into the system, accepted for processing, and properly reflected in the system output. As a result, HUD may not have been aware of all IT problems reported by users and was unable to ensure that issues not recorded were resolved or escalated when necessary.

HUD Had Begun To Consider Solutions

According to HUD, it was evaluating a different help desk solution and intended to transition away from its current system. However, HUD had not completed actions needed to address the weaknesses in its current system and did not yet have a timeline for when it could potentially transition to a different help desk solution.

Conclusion

The integrity of information system data is of utmost importance, and organizations should reasonably ensure that data are complete, accurate, and valid. HUD's national help desk system lacked adequate controls to ensure the completeness and validity of data. Although HUD stated that it was evaluating a different help desk solution, the issues identified are ongoing and continue to impact HUD's ability to ensure that IT problems reported by users are captured, resolved, and escalated when necessary. Additionally, inadequate controls over ticket data can erode user confidence in HUD's national help desk system.

Recommendations

We recommend that the Office of the Chief Information Officer

- 4A. Assess its help desk system against other technical solutions and ensure that the help desk solution used captures complete data on technical support requests. This measure includes but is not limited to ensuring that sequence gaps are properly documented or do not occur, valid transactions are accepted by the help desk system, rejected transactions are identified, and the history of each transaction is retained.

Scope and Methodology

We conducted the audit between July 2020 and June 2022, both remotely and at HUD's headquarters in Washington, DC. The initial audit period covered March through November 2020 and was expanded in June 2022 to include updates on HUD's telework status as well as information provided by HUD on actions it had taken and planned to take to address the weaknesses identified during the initial audit period.

Our audit was based on the U.S. Government Accountability Office's Federal Information System Controls Audit Manual (FISCAM) methodology. FISCAM provides a methodology for performing information system (IS) control audits in accordance with generally accepted government auditing standards (GAGAS) when IS controls are significant to the audit objectives. As defined in GAGAS, IS controls consist of those internal controls that are dependent on information systems' processing and include general controls and application controls.

To assess HUD's IT infrastructure's preparedness and capability to support extensive mandatory telework during the COVID-19 pandemic, we

- reviewed relevant criteria, including OMB memorandums, NIST special publications, and Federal Information Processing Standards;
- identified and reviewed HUD's IT security policies and procedures and other relevant guidance distributed to HUD staff;
- analyzed the national help desk data for 55,291 tickets created between March 1, 2020, and June 30, 2020; and
- surveyed and held discussions with HUD personnel.


We conducted the audit in accordance with GAGAS. 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 objective(s). We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Appendixes

APPENDIX A - AUDITEE COMMENTS AND OIG'S EVALUATION

Ref to OIG Evaluation – Auditee Comments

Attached to HUD's memorandum was an excel attachment that included their detailed comments. We are not including the entirety of the attachment provided by HUD because it included points of contact and other sensitive information. On the next page, we have extracted HUD's comments from the excel attachment and in cooperation with HUD, removed or summarized sensitive information that was included.



U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
WASHINGTON, D.C. 20410-3000

CHIEF INFORMATION OFFICER

December 12, 2022

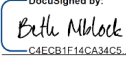
MEMORANDUM FOR: Kilah S. White, Assistant Inspector General for Audit, GA

FROM: Beth Niblock, Chief Information Officer

SUBJECT: HUD comments to Draft FY 23 Assessment of HUD's IT Infrastructure to Support Extensive Telework Support Report (2023-FO-XXXX)

This memorandum is in response to the Office of the Inspector General (OIG) draft report Draft FY 23 Assessment of HUD's IT Infrastructure to Support Extensive Telework Support Report (2023-FO-XXXX). The Office of the Chief Information Officer (OCIO) has carefully reviewed the Draft Report and provided comments.

If you have questions or require additional information, please contact Paul Scott, Business Change and Integration Officer, OCIO, at (202) 402-2354 (paul.a.scott@hud.gov), or Porter Davis, Audit Liaison Officer, at (202) 402-6114 (porter.b.davis@hud.gov).

DocuSigned by:

Beth Niblock
Chief Information Officer
Department of Housing and Urban Development

12/12/2022
Date

Attachments:

- HUD comments to Draft FY 23 Assessment of HUD's IT Infrastructure to Support Extensive Telework Support Report (2023-FO-XXXX) [Link to Attachment](#)

cc:

Russel Ramos, Acting Chief Information Security Officer, QS
Ivo Djoubraïlov, Acting Chief Technology Officer, QS
Bridget Carper, Acting Deputy CIO, Customer Relationship and Performance, QS
Rhonda Press, Acting CIO, Business and IT Resource Management Office, OCIO, QS
Juan C. Sargeant, Deputy CIO, Infrastructure and Operations Office, QS
Helen McBride, Senior Adviser, Office of the Chief Information Officer, Q
Jacqueline Hyslop, Office of Inspector General for Audit
Sarah Sequeira, Office of Inspector General for Audit
Brittany Wing, Audit Director, Office of Inspector General for Audit
Kilah White, Assistant Inspector General for Audit

Reference to OIG Evaluation	Auditee Comments (Auditee comments below have been extracted from HUD’s excel attachment and in cooperation with HUD, we removed or summarized sensitive information)
Comment 1	<p>IOO concurs to some extent with the first finding regarding security patches for HUD’s computers, we cannot concur with the sentence in the third sentence of page 6’s first paragraph stating “more than two-thirds of HUD’s computers” since HUD’s computers consist of servers, laptops, desktops, and mobile devices. In the 4th sentence of the same paragraph, OIG states the VPNs bandwidth as the point of failure for patching remote devices due to the number of simultaneous connections, however the issue was due to users disconnecting from the VPN, not connecting to the VPN, and/or disconnecting when laptop performance decreased as patches were being applied. At the start of the pandemic OCIO increased the number of VPN licenses and separated those licenses to enable half the HUD population to access VPN from one Data Center while the others accessed was limited to the secondary Data Center, while simultaneously upgrading the circuits to a 10 GB backbone in each data center to support the increased capacity. IOO also does not concur with the 5th sentence in the paragraph that states software was outdated. IOO concurs with OIGs assessment that additional improvements are needed, and IOO has already taken actions to address the issue.</p>
Comment 2	<p>On page 6, paragraph 2, OIG states that HUD failed to update nearly 5,100 HUD computers within 200 days, and as previously stated, IOO has since taken actions to mitigate the issues with applying patches to remote devices by implementing split tunneling. Furthermore, IOO is in the process of taking additional actions.</p>
Comment 3	<p>On page 6, paragraph 4, OIG again asserts HUD had not patched two-thirds of its computers, but in the preceding paragraph OIG implies HUD’s computers consists of servers and workstations, yet according to OIG only ~5,100 laptops/workstations were not patched, which is significantly less than HUD’s computers when servers, workstations, and mobile devices are included as part of HUD’s computers. OIG continues the same vain in the same paragraph as it moves into page 7, asserting the VPN as the cause for the issue, and as IOO stated earlier, the cause is inaccurate.</p>
Comment 4	<p>On page 8, first paragraph, OIG states HUD’s improvements have not resolved the weaknesses, however, the actions taken negated all issues associated with bandwidth utilization impacting user experiences, and the 10 GB backbone further negated bandwidth utilization issues.</p>
Comment 5	<p>IOO does not concur with OIG’s finding number 2 on page 9, paragraph 1 asserting HUD’s network performance issues on HUD’s VPN, and their reference to increased tickets on page 9 paragraph 2. While HUD had increase in tickets regarding network access during the months of March and June 2020, over 95% of the tickets were questions from the users on how to connect to the network, most of the remaining tickets were due to the user’s home network ISP service providers. Users across the nation experienced poor network performance as network traffic across the nation</p>

	<p>increased as all employees and students began working remotely and consuming available bandwidth. Multiple daily/weekly reports on HUD’s bandwidth utilization showed limited periods when more than 80% of HUD’s available bandwidth at any data center was being consumed. In addition, HUD’s review of the tickets shows 4,601 tickets during the stated period of March 2020 to June 2020, not OIG’s assertion of 5,949.</p>
Comment 6	<p>IOO concurs with Finding 3.</p>
Comment 7	<p>IOO does not concur with finding number 4 regarding the national help desk system not capturing all data. On page 15, second paragraph, OIG asserts HUD’s ticketing system is missing approximately 5,800 tickets, however those missing sequence numbers are based on whether duplicate tickets were deleted, or a user/staff member began creating a ticket but neglected to save the ticket which would bypass the number that was assigned at the beginning of the ticket creation process. HUD has the ability to run a report showing the number of tickets that were removed from the sequencing based on deletions or incomplete processing.</p>

OIG Evaluation of Auditee Comments

- Comment 1 In the final report, we clarified the verbiage for *“more than two-thirds of HUD’s computers”* to say, *“laptops and desktops”* (to illustrate servers and mobile devices were excluded). We disagree that the cause as stated within the report is inaccurate. We concluded during our audit that the delay in security updates occurred because of (1) the significant increase of users accessing the network simultaneously during mandatory telework and (2) VPN capacity limitations. HUD agreed with our conclusions during the audit and expressed concerns about the full workforce needing to be on the VPN to complete the updates and user’s inability to perform their work if they were unable to connect to the local network to have their computers serviced and updated. Regarding the comment on *“outdated software”*, we clarified in the report that the *“computers had not received the security updates”* instead of saying the *“software was outdated.”*
- Comment 2 We agree that HUD informed OIG that actions to mitigate the issues are underway. OIG has noted that in the report under the section titled *“HUD Had Begun To Address the Weaknesses But More Improvements are Needed.”* Specifically, this section states that HUD said it began increasing network capacity which enabled it to process computer security updates for HUD staff when working remotely. In June 2022, HUD informed us that they planned to implement additional improvements, which we also noted within the report. However, since these plans were not executed during our audit, HUD OIG has not confirmed the actions HUD reported taking after the audit work concluded. We look forward to working with the OCIO through the audit resolution process.
- Comment 3 We clarified our report to illustrate that our results relating to HUD laptops and desktops, excluded servers and mobile devices. The cause was not changed and remains as stated, that the bandwidth was not sufficient to accommodate the significant increase in the number of users accessing the network simultaneously during mandatory telework.
- Comment 4 Within the report we incorporated information provided by the OCIO on the status of its corrective actions as of June 2022. As part of the audit resolution process, HUD will decide the types of evidence or documentation to support the actions taken/to be taken to address the weaknesses cited. HUD OIG has not confirmed that *“the actions taken negated all issues...”* We look forward to working with the OCIO through the audit resolution process.

- Comment 5 Based on the evidence provided to us during the audit, we do not agree with the statement that *“HUD’s review of the tickets shows 4,601 tickets during the stated period of March 2020 to June 2020...”*. We also do not agree with the assertion that *“over 95% of the tickets were questions from the users on how to connect to the network, most of the remaining tickets were due to the user’s home network ISP service providers...”*. The help desk ticket documentation reviewed during our audit was provided by HUD. The documentation we reviewed reflected 5,949 tickets with many VPN related issues. Our assessment and classification of the tickets was provided to HUD during the audit and HUD did not refute our results or provide additional documentation supporting different results at that time.
- Comment 6 We acknowledge the OCIO agreement with Finding 3 and look forward to working with the OCIO through the audit resolution process.
- Comment 7 The Help desk tickets we received during the audit did not have any information about tickets missing (i.e., gaps) sequence numbers. We do agree that the ticket gaps could have resulted from deletion and or incomplete processing. In addition, during the audit we specifically requested information on the ticket numbers included in the gaps we identified; however, HUD did not provide additional documentation to support the ticket gaps. Therefore, Finding 4 was not changed and we look forward to working with HUD OCIO during the audit resolution process.