U.S. SMALL BUSINESS ADMINISTRATION OFFICE OF INSPECTOR GENERAL

Undetected Vulnerabilities from Personally Owned Devices

Management Advisory

Report 25-11

April 22, 2025

Make a Difference

To report fraud, waste, or mismanagement, contact the U.S. Small Business Administration's Office of Inspector General Hotline at https://www.sba.gov/oig/hotline. You can also write to the U.S. Small Business Administration, Office of Inspector General, 409 Third Street, SW (5th Floor), Washington, DC 20416. In accordance with the Inspector General Act of 1978, codified as amended at 5 U.S.C. §§ 407(b) and 420(b)(2)(B), confidentiality of a complainant's personally identifying information is mandatory, absent express consent by the complainant authorizing the release of such information.

NOTICE:

Pursuant to the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Public Law 117-263, Section 5274, any nongovernmental organizations and business entities identified in this report have the opportunity to submit a written response for the purpose of clarifying or providing additional context as it relates to any specific reference contained herein. Comments must be submitted to AIGA@sba.gov within 30 days of the final report issuance date. We request that any comments be no longer than two pages, Section 508 compliant, and free from any proprietary or otherwise sensitive information. The comments may be appended to this report and posted on our public website.

OFFICE OF INSPECTOR GENERAL
U.S. SMALL BUSINESS ADMINISTRATION

MEMORANDUM

Date: April 22, 2025

To: Kelly Loeffler
Administrator

From: Sheldon Shoemaker
Deputy Inspector General
Sheldon Shoemaker

Subject: Management Advisory on Undetected Vulnerabilities from Personally Owned Devices (Report 25-11)

The Office of Inspector General (OIG) is issuing this management advisory to bring to your attention possible security threats from personally owned devices accessing the U.S. Small Business Administration (SBA) information technology (IT) network from national and international locations with only a username and password.

We identified in our fiscal years 2023 and 2024 Federal Information Security Modernization Act (FISMA) assessments that SBA did not have multifactor authentication enabled for users to access the agency's secure network. Multifactor authentication is a high security control that requires a username, password, and an identity card, unique security code, or biometrics to access a system. Relying on usernames and passwords alone greatly increases the risk of SBA data being accessed and exploited by cyber criminals and other bad actors. We also determined personally owned devices could access the SBA network from foreign locations, which is prohibited by SBA IT policy. SBA's information systems are more vulnerable to unauthorized access that could exploit sensitive agency information.

We considered management comments on the draft of this report when preparing the final report. SBA management agreed with all five recommendations, and they have all been resolved.

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Christina Sweet, Acting Director, Information Technology and Financial Management Group, at (202) 205-8992 or Andrea Deadwyler, Assistant Inspector General for Audits, at (202) 205-6586.

cc: Wesley Coopersmith, Chief of Staff, Office of the Administrator
Ben Grayson, Deputy Chief of Staff, Office of the Administrator
Robin Wright, Chief Operating Officer, Office of the Administrator
Douglas Robertson, Acting Chief Information Officer, Office of the Chief Information Officer
Nathan Davis, Chief Financial Officer and Chief Risk Officer, Office of Performance, Planning, and the Chief Financial Officer
Deborah Chen, Deputy Chief Financial Officer, Office of Performance, Planning, and the Chief Financial Officer
Anna Maria Calcagno, Director, Office of Strategic Management and Enterprise Integrity
Wendell Davis, General Counsel, Office of General Counsel
Michael Simmons, Attorney Advisor, Office of General Counsel

Contents

Appendices

Background

In December 2024, the Office of Inspector General (OIG) identified that the U.S. Small Business Administration (SBA) unknowingly allowed personally owned devices, such as smartphones, laptops, or tablet computers, to access, store, and transmit agency data with only a username and password from national and international locations. Shadow information technology (IT) is any software, hardware, or IT asset used on a network without the IT department's approval, knowledge, or oversight. Shadow IT must be controlled because it creates blind spots, which means the agency incurs risks without management's knowledge. Personally owned devices are a form of shadow IT. They can open the agency up to IT security risks, such as unauthorized access and theft of personally identifiable information, that can be exploited by cyber criminals and other bad actors. Cyber threats include, but are not limited to, disclosure of sensitive data, unauthorized changes, or backdoor access to other network resources.

The agency has been vulnerable to cybersecurity threats from foreign Internet Protocol (IP) addresses in the past although it has made improvements in this area. In 2022, OIG reported on the danger of international cyber criminals and other bad actors gaining access to SBA systems.[1] Millions of attempts were made to submit Coronavirus Disease 2019 (COVID-19) Economic Injury Disaster Loan (EIDL) applications from foreign IP addresses. SBA stopped most of them; however, we found the agency still approved and disbursed 41,638 COVID-19 EIDLs, advances, and grants totaling $1.3 billion.

We also identified in our fiscal years 2023 and 2024 Federal Information Security Modernization Act (FISMA) assessments that SBA did not have multifactor authentication enabled for users to access the agency's secure network. Multifactor authentication is a key security control that requires a username, password, and an identity card, unique security code, or biometrics to access a system.

The SBA Office of the Chief Information Officer (OCIO) manages the agency's information security and privacy program. OCIO's responsibilities are to implement a zero trust architecture,

[1] SBA OIG, Report 22-17, *COVID-19 Economic Injury Disaster Loan Applications Submitted from Foreign IP Addresses* (September 12, 2022).

which focuses on protecting the network. A zero trust architecture ensures inherent trust to the network is not granted to IT assets such as personal mobile devices. Verifying a user and their device, and what they can access must be established first before entry to the network is granted.

An executive order on improving the nation's cybersecurity states the federal government must modernize its approach to cybersecurity, including increasing the federal government's visibility into threats. It also states the federal government must adopt security best practices, advance toward a zero trust architecture, and secure cloud services.[2] SBA uses cloud computing services, which means employees can access its data remotely from an online portal.

Users Can Gain Unauthorized Access to the SBA Network Using Personally Owned Devices

The SBA network is exposed to unauthorized access through an unsecured entry point. Agency procedures state that access to the SBA network must be restricted to secure methods.[3]

Multifactor Authentication

On December 6, 2024, OIG determined personally owned devices can access SBA's network using the online cloud service portal without multifactor authentication. We promptly informed agency management of the network security vulnerability. Although the agency uses software to secure access to the network for Windows-system devices, the software does not restrict other mobile devices. As a result, agency management was not alerted of the security vulnerability. A similar issue was identified in the fiscal years 2023 and 2024 FISMA assessments. Specifically, authorized users can access the network without personal identity verification (PIV) cards.

Agency managers stated they are working on a remediation plan. Without multifactor authentication, every personally owned device that connects to the network is a potential cyber

[2] Executive Order No. 14028, 86 Fed. Reg. 26633 (May 12, 2021).

[3] SBA, Standard Operating Procedure 90 47 6, Cybersecurity and Privacy Policy (March 28, 2022).

threat. Cyber threats from personally owned devices include but are not limited to unauthorized changes, device loss or theft, backdoors to access other network resources, or disclosure of sensitive data that can be stored, downloaded or printed. Agency procedures state that access to sensitive data must be from government issued equipment. Further, sensitive data should not be downloaded, stored, or printed on personally owned devices. In addition, agency managers should use identification and authentication methods that detect intrusion attempts and unauthorized access as required by the Office of Management and Budget (OMB)[4] and agency procedures[5].

Access from Foreign IP Addresses

We determined that users could access the SBA network via the Microsoft 365 portal from a foreign IP address. SBA managers responded and manually blocked the user approximately 2 days later. Although access to the network was stopped in this specific instance for one user, the vulnerability still exists. The vulnerability occurred because the security software the agency uses should have automatically prevented the user from gaining entry to network resources on all attempts. The agency has been vulnerable to cybersecurity threats from foreign IP addresses in the past. Agency procedures state users shall not access SBA resources requiring authentication from any foreign location unless they are performing official government duties or on official government travel[6]. Cybersecurity threats such as cyber criminals, malware that evades security systems, undetected unauthorized access to a network, or more can occur through unpermitted access from foreign countries to harm the agency and its mission. Agency managers stated they are working on a remediation plan to prevent network access from foreign countries.

[4] OMB, M-22-01, “Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response” (October 8, 2021).

[5] SBA, Standard Operating Procedure 90 47 6, Cybersecurity and Privacy Policy (March 28, 2022).

[6] SBA, Standard Operating Procedure 90 47 6, Cybersecurity and Privacy Policy (March 28, 2022).

Recommendations

We recommend the Administrator direct the Associate Administrator for the Office of the Chief Information Officer to:

Recommendation 1: Ensure personally owned devices use multifactor authentication as required by SOP 90 47 6.

Recommendation 2: Ensure all personal devices connecting remotely to SBA's network have updated anti-malware software running with the latest signature files, a firewall installed and running, and all security patches installed as required by SOP 90 47 6.

Recommendation 3: Ensure that appropriate security, including encryption, application controls, password usage, remote locking, remote wiping, and operating system protection can be enforced for mobile devices as required by SOP 90 47 6.

Recommendation 4: Restrict users from connecting to SBA systems from international IP addresses as required by SOP 90 47 6.

Recommendation 5: Implement or enhance current real-time continuous monitoring of mobile phone and personal computer data with rules-based automated response and analysis capabilities as required by OMB M-22-01.

Evaluation of Agency Response

Management provided formal written comments that are included in their entirety in Appendix 1. Additionally, management responded to the report in Integrity, SBA's audit management system, which included whether management agreed with the recommendations and the target dates for implementing the corrective actions. Management agreed with all five recommendations. Management implemented corrective actions that were sufficient to close four of the recommendations. In addition, management's planned actions are sufficient to resolve the remaining recommendation.

Summary of Actions Necessary to Close the Recommendations

The following section summarizes the status of our recommendations and the actions necessary to close them.

Recommendation 1

Ensure personally owned devices use multifactor authentication as required by SOP 90 47 6.

Status: Closed

SBA management agreed with the recommendation, stating that SBA no longer allows personal devices to connect remotely to its systems. Management stated they plan to implement the corrective action by April 30, 2025. On April 14, 2025, management provided evidence that they blocked personal devices from accessing its systems. Management demonstrated that SBA no longer allows personal devices to connect remotely to its systems, thereby mitigating the risk of unauthorized access to the network. We consider this recommendation closed.

Recommendation 2

Ensure all personal devices connecting remotely to SBA's network have updated anti-malware software running with the latest signature files, a firewall installed and running, and all security patches installed as required by SOP 90 47 6.

Status: Closed

SBA management concurred with our recommendation, stating they no longer allow personal devices to connect remotely to its systems. Management plans to implement the corrective action by April 30, 2025. Management provided documentation that personal devices are unable to connect remotely to the SBA systems on April 14, 2025. We consider this recommendation closed.

Recommendation 3

Ensure that appropriate security, including encryption, application controls, password usage, remote locking, remote wiping, and operating system protection can be enforced for mobile devices as required by SOP 90 47 6.

Status: Closed

SBA management agreed with the recommendation, stating that SBA no longer allows personal devices to connect remotely to its systems. Management stated they plan to implement the corrective action by April 30, 2025. On April 14, 2025, management provided evidence that they blocked personal devices from accessing SBA's systems. The OIG reviewed the documentation and determined that SBA no longer allows personal devices to connect remotely to its systems. This recommendation is considered closed.

Recommendation 4

Restrict users from connecting to SBA systems from international IP addresses as required by SOP 90 47 6.

Status: Closed

SBA management agreed with the recommendation, stating that SBA no longer allows personal devices to connect remotely to its systems. Management stated they plan to implement the corrective action by April 30, 2025. Management demonstrated that personal devices cannot connect remotely to the SBA systems as of April 14, 2025, based on documentation managers provided. We consider this recommendation closed.

Recommendation 5

Implement or enhance current real-time continuous monitoring of mobile phone and personal computer data with rules-based automated response and analysis capabilities as required by OMB M-22-01.

Status: Resolved

SBA management agreed with the recommendation, stating that personal devices are no longer allowed to connect remotely to SBA systems. SBA managers stated they have developed policies for device compliance, app protection, and conditional access for all government-furnished phones and devices. In addition, management also stated SBA-issued mobile devices, including phones, are secured, scanned for threats, and provide alerts of threat-level data to SBA managers. Management stated they plan to implement the corrective action by April 30, 2025. Management demonstrated that they blocked personal devices from accessing its systems based on documentation they provided. OIG reviewed the evidence and determined that it was sufficient to address the corrective action plan. Specifically, OIG determined that SBA no longer allows personal devices to connect remotely to its systems.

This recommendation can be closed when management provides evidence that they implemented policies to monitor SBA-issued mobile devices.

Scope and Methodology

The overall objective of our management advisory was to determine if shadow IT risks in the mobile systems environment are mitigated in accordance with organizational and federal requirements and guidance. In addition, we wanted to bring to management's attention possible security threats from personally owned devices accessing the SBA IT network from national and international locations with only a username and password. During our review, we found unauthorized access to the network through personally owned mobile devices was not blocked from international IP addresses. In addition, multifactor authentication was not enforced for the personal mobile devices accessing the network. This management advisory brings attention to concerns that non-government furnished equipment, personally owned equipment, can gain entry to the SBA network from national and international locations with only a user ID and password.

We reviewed federal laws, regulations, policies, and procedures. We interviewed Office of the Chief Information Officer program officials and reviewed supporting documentation to gain an understanding of the vulnerability. We prepared this management advisory in alignment with OIG's quality control standards and the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Federal Offices of Inspector General,* which require that we conduct our work with integrity, objectivity, and independence. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions.

Appendix 1: Agency Response

U.S. Small Business Administration
Response to Draft Report

U.S. SMALL BUSINESS ADMINISTRATION
WASHINGTON, D.C. 20416

To: Sheldon Shoemaker
Deputy Inspector General

From: Douglas Robertson
Chief Information Officer (Acting)

Date: April 1, 2025

Subject: Response to Undetected Vulnerabilities from Personally Owned Devices

We appreciate the Office of Inspector General's (OIG) role in providing guidance to SBA management to help ensure that our programs are effectively managed, and for the feedback provided in this draft report.

SBA no longer allows the use of Personally Owned Devices on our network, and we feel that this issue is no longer in existence. We will update our Policy accordingly, to state we no longer allowed Personally Owned Devices, but in the meantime OCIO is providing the appropriate documentation to close out the findings.

Recommendation 1 - Ensure personally owned devices use multifactor authentication as required by SOP 90 47 6.

SBA Response - SBA no longer allows personal devices to connect remotely. Screenshots show the Mobile Device Management Policy has been updated to block personal devices. Also, screenshots have been provided showing that a user's personal iPhone was being blocked.

Recommendation 2 - Ensure all personal devices connecting remotely to SBA's network have updated anti-malware software running with the latest signature files, a firewall installed and running, and all security patches installed as required by SOP 90 47 6.

SBA Response - SBA no longer allows personal devices to connect remotely. Screenshots show the Mobile Device Management Policy has been updated to block personal devices. Also, screenshots have been provided showing that a user's personal iPhone was being blocked.

Recommendation 3 - Ensure that appropriate security, including encryption, application controls, password usage, remote locking, remote wiping, and operating system protection can be enforced for mobile devices as required by SOP 90 47 6.

SBA Response SBA no longer allows personal devices to connect remotely. Screenshots show the Mobile Device Management Policy has been updated to block personal devices. Also, screenshots have been provided showing that a user's personal iPhone was being blocked.

Recommendation 4 - Restrict users from connecting to SBA systems from international IP addresses as required by SOP 90 47 6.

SBA Response - SBA no longer allows personal devices to connect remotely. Screenshots show the Policy has been updated to block personal devices. Also, screenshots have been provide showing a user's personal iPhone being blocked.

Recommendation 5 - Implement or enhance current real-time continuous monitoring of mobile phone and personal computer data with rules-based automated response and analysis capabilities as required by OMB M-22-01.

SBA Response - SBA no longer allows personal devices to connect remotely. SBA Mobile devices including phones are secured, enforce, and scanned with MS Intune with alerts going to Microsoft Defender. SBA scans mobile devices through Intune, which is integrate with Mobile Threat Defense (MTD) in our Azure environment, which actively scan devices for threats and provide threat level data to Intune we have developed policies like device compliance, app protection, and Conditional Access for all phones and devices

DOUGLAS
ROBERTSON

Digitally signed by
DOUGLAS ROBERTSON
Date: 2025.04.07
08:04:17 -04'00'

Douglas Robertson
Chief Information Officer (Acting)