OFFICE OF INSPECTOR GENERAL
U.S. Agency for International Development

USAID Needs To Improve Policy and Processes To Better Protect Information Accessed on Personal Devices

AUDIT REPORT A-000-20-006-P
JUNE 19, 2020

1300 Pennsylvania Avenue NW • Washington, DC 20523
https://oig.usaid.gov • 202-712-1150

The Office of Inspector General provides independent oversight that promotes the efficiency, effectiveness, and integrity of foreign assistance provided through the entities under OIG's jurisdiction: the U.S. Agency for International Development, Millennium Challenge Corporation, U.S. African Development Foundation, and Inter-American Foundation.

Report waste, fraud, and abuse

USAID OIG Hotline
Email: ig.hotline@usaid.gov
Complaint form: https://oig.usaid.gov/complainant-select
Phone: 202-712-1023 or 800-230-6539
Mail: USAID OIG Hotline, P.O. Box 657, Washington, DC 20044-0657

MEMORANDUM

DATE: June 19, 2020

TO: USAID/Bureau for Management, Chief Information Officer, Jay Mahanand

FROM: USAID OIG Deputy Assistant Inspector General for Audit, Alvin Brown /s/

SUBJECT: USAID Needs To Improve Policy and Processes To Better Protect Information Accessed on Personal Devices (A-000-20-006-P)

This memorandum transmits the final report on our audit of USAID staff's use of personal devices to access an Agency external cloud system. Our audit objective was to determine whether USAID implemented key internal controls to protect information available in the external cloud system when accessed through staff's personal devices based on controls recommended by the National Institute of Standards and Technology, Digital Services Advisory Group, and Federal Chief Information Officers Council. Specifically, we assessed (1) USAID's implementation of key internal controls related to access, identification and authentication, system and communications protection, roles and responsibilities, education, privacy, ethics and legal concerns, devices and applications, and asset management and (2) factors that may have affected USAID's implementation of these controls. In finalizing the report, we considered your comments on the draft and included them in their entirety, excluding attachments, in appendix B.

The report contains four recommendations to improve USAID's control environment to protect information available in the external cloud system when accessed through staff's personal devices. After reviewing the information that you provided in response to the draft report, we consider three closed (recommendations 1, 2, and 4), and one resolved but open pending completion of planned activities (recommendation 3).

For recommendation 3, please provide evidence of final action to the Audit Performance and Compliance Division.

We appreciate the assistance you and your staff extended to us during this audit.

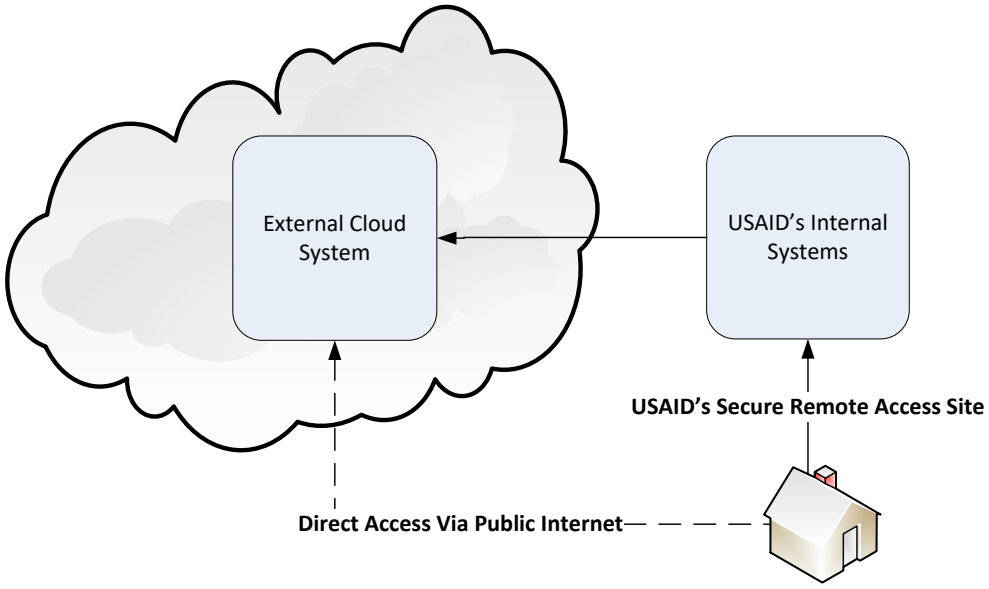
CONTENTS

INTRODUCTION

USAID staff rely on both the Agency's internal computing systems and external cloud computing systems to conduct their daily business.[1] While USAID has various cloud computing systems, only one external system is the focus of this audit (referred to as "the external cloud system"). This system has a set of web applications that includes email, shared calendars, and videoconferencing as well as tools and software to create, edit, store, and share documents in browsers and across devices. However, misuse or unauthorized access to this external cloud system may critically harm the integrity of USAID's operations by allowing hackers to obtain access to its information and systems.

Given that cell phones and other personal devices have become indispensable tools for today's workforce, USAID staff can access the Agency's external cloud system from both Government-issued and personal devices when working remotely.[2] As shown in figure 1, staff can access this system whether they use the Agency's secure remote access site or log in directly through the public Internet.

Figure 1. Access to USAID's External Cloud System



Source: OIG, based on the external cloud system's security plan.

While the secure remote access site provides security controls when using personal devices to access the external cloud system, the direct access method significantly relies on controls implemented on the user's device, if any. Therefore, having appropriate

[1] For this report, the term "staff" refers to all labor categories, including direct hires and contractors, at all levels within the Agency.

[2] Personal devices are staff-controlled technologies, such as computers, smartphones, and tablets, that are outside the Agency's control and not owned by the Government.

security controls in place when staff use personal devices is critical for reducing the risk of unauthorized access, disclosure, and modification of the Agency's data, including sensitive but unclassified information.

The audit objective was to determine whether USAID implemented key internal controls to protect information available in the external cloud system when accessed through staff's personal devices based on controls recommended by the National Institute of Standards and Technology, Digital Services Advisory Group, and Federal Chief Information Officers Council. Specifically, we assessed (1) USAID's implementation of key internal controls related to access, identification and authentication, system and communications protection, roles and responsibilities, education, privacy, ethics and legal concerns, devices and applications, and asset management and (2) factors that may have affected USAID's implementation of these controls.

To conduct our work, we reviewed USAID's policies, procedures, the external cloud system's services contract, and other applicable documentation regarding the selected internal controls. We also interviewed Agency officials in the Office of the Chief Information Officer (OCIO), including the chief information officer and the external cloud system's primary administrator. We surveyed a nonstatistical sample of USAID's external cloud system users to assess their use of the application. In addition, we reviewed the status of external cloud system accounts for a sample of separated staff. We also performed independent tests of controls, such as session termination, session lock, authentication, and system and communications protection. We conducted our work in accordance with generally accepted government auditing standards. Appendix A provides more detail on our scope and methodology.

SUMMARY

USAID had a risk of an information security breach due to its use of the external cloud system. We found that the Agency had some internal controls in place to address the risk. For example, USAID required staff to take training in protecting sensitive information and to sign a user agreement. It also required staff using personal devices to log into their external cloud system accounts using Agency-issued RSA tokens. [3] Yet, the Agency faced an increased risk of a breach because it had not implemented key internal controls needed to protect information accessed in the external cloud system by staff on their personal devices. Specifically, USAID did not fully implement key controls related to (1) access controls, (2) roles and responsibilities, (3) ethics and legal concerns, (4) asset management and privacy, and (5) devices and applications. For example, in regard to access controls, USAID did not implement controls to

[3] An RSA token is a device, either physical ("hard") or an application on a user's mobile device ("soft"), that provides users with a passcode to access their USAID e-mail and desktop when teleworking via server-based computing (SBC/Citrix). USAID, Mandatory Reference for ADS chapter 545, "Guidelines for Remote Access Soft Tokens for Personal Devices," November 9, 2012.

automatically terminate user sessions after 60 minutes of inactivity, as required by Agency policy. It also did not always identify or cancel the external cloud system user accounts for contractors when the accounts were no longer required.

We identified four reasons that USAID did not implement the key controls. The Agency did not:

1. Have clear policies to restrict or provide procedures on how staff should use their personal devices to access Agency information and systems, such as a bring your own device (BYOD) program;
2. Perform a risk assessment on the use of personal devices for remote access to USAID information and systems so the Agency could implement controls to mitigate any unacceptable risks that may be identified;
3. Implement automated protection to prevent staff from logging directly into their Agency accounts on personal devices outside of the Agency's secure remote access site; and
4. Have effective procedures and consistent policies for notifying network administrators when contractors no longer needed access to Agency systems.

We are making four recommendations to improve USAID's control environment to protect information available in the external cloud system when accessed through staff's personal devices.

BACKGROUND

For many organizations, employees and contractors use enterprise telework or remote access technologies to perform work from external locations. All components of these technologies, including organization-issued and personal devices, should be secured against expected threats as identified through threat models.

Allowing the use of personal devices to access systems and implementing a BYOD program present Government agencies with a "myriad of security, policy, technical, and legal challenges" to internal communications, relationships, and trust with external partners.[4] For example, agencies need to ensure that they have rules in place for what employees can and cannot do with Government information on personally owned devices and that staff agree to let agencies examine those devices if needed.

Implementing a BYOD program on an external cloud system presents even more challenges. For example, in March 2015, USAID OIG identified instances where the permissions of users in the external cloud system were inadequate for protecting sensitive information from being shared improperly.[5] Therefore, an agency must be

[4] Digital Services Advisory Group and Federal Chief Information Officers Council, "A Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs," August 23, 2012.
[5] USAID OIG, "Audit of USAID's Progress in Adopting Cloud Computing Technologies" (A-000-15-006-P), March 12, 2015.

proactive in implementing its own configuration and controls, as there are shared responsibilities among the external cloud system, the cloud service providers, and the customer agencies.[6] Specifically, customer agencies have the responsibility to assess, implement, and monitor specific controls for their respective use of the external cloud system services.

To address the potential security risks relating to the use of personal devices, the National Institute of Standards and Technology (NIST) recommends a variety of security controls.[7] Specifically, it lists those that are most pertinent for securing enterprise telework, remote access, and BYOD technologies. For example, in order to confirm that the person using remote access is authorized, many organizations require teleworkers to reauthenticate periodically during remote access sessions, such as after 8 hours of a session or after 30 minutes of idle time.

According to NIST, organizations should assume that (1) hostile threats will attempt to gain access to their information and systems, (2) teleworkers' devices—particularly prone to loss or theft—will be acquired by malicious parties who will attempt to recover sensitive information or gain access to their network, and (3) communications on external networks are susceptible to eavesdropping, interception, and modification. Therefore, it is critical for agencies to establish a strong control environment over all methods of remote access.

USAID IMPLEMENTED SOME KEY CONTROLS, BUT ADDITIONAL ACTIONS ARE NECESSARY TO PROTECT INFORMATION ACCESSED ON PERSONAL DEVICES

USAID had internal controls in place for identification and authentication, system and communications protection, education, privacy, and devices and applications—all of which are identified as pertinent security controls for remote access.[8] In some cases, USAID took action to address control gaps we identified in the course of our audit work. Specifically, USAID had the following controls in place at the end of audit fieldwork:

- *Identification and authentication.* USAID required that when users log into their external cloud system accounts on personal devices, they must use Agency-issued

[6] These responsibilities are documented in the U.S. General Services Administration's FedRAMP security package for this external cloud system.
[7] NIST is responsible for developing information security standards and guidelines, including minimum requirements for Federal information systems. Its recommendations for security controls are contained in NIST Special Publication (SP) 800-46, Revision 2, "Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security," July 2016.
[8] NIST's "Guide to Enterprise Telework, Remote Access, and BYOD Security" and the Digital Services Advisory Group and Federal Chief Information Officers Council's "A Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs."

RSA tokens, whether they log in via the secure remote access site or directly from the public Internet (opening a web browser and going to the external cloud system's public website).

- *System and communications protection.* At initial review, the external cloud system did not have controls in place to protect communications, nor did OCIO have mitigating controls in place. However, during the course of our audit, the service provider of the external cloud system fixed the secure connection of browsers and transmission of emails. In addition, we tested and confirmed that it is not possible to connect to the external cloud system on personal devices without the NIST-approved encryption strength.[9]

- *Education.* USAID policies required staff to take training in protecting personally identifiable information, which informs users of current policies outlining the acceptable use of systems. Also, USAID required staff to sign a network access user agreement before allowing access to Agency systems. The user agreement informs staff that they are required to abide by all USAID policies and guidelines to protect USAID systems from misuse, abuse, loss, or unauthorized access.

- *Privacy.* At initial review, USAID did not clearly communicate whether users should expect privacy when using Agency systems. However, during the course of our audit, the Agency implemented policies to alert users that by entering the USAID network and systems, they have no reasonable expectation of privacy.

- *Devices and applications.* During the course of our audit, the Agency issued policies to alert users of the USAID network and systems with a warning banner that they were accessing a U.S. Government information system. In addition, USAID's policies prohibited users from storing sensitive Agency content on personal devices.

However, USAID did not implement key controls related to access controls, roles and responsibilities, ethics and legal concerns, asset management and privacy, and devices and applications—all of which are identified as pertinent security controls for remote access.[10] Specifically, USAID did not have the following controls in place:

Access controls

Access controls include (1) terminating a session, where the information system automatically terminates a user session after an organization-defined time period; (2) locking a session, where the information system initiates a lock after an organization-defined period of inactivity; (3) managing, disabling, and removing information system

[9] The NIST-approved encryption strength is transport layer security (TLS). TLS is a protocol created to provide authentication, confidentiality, and data integrity between two communicating applications.

[10] NIST's "Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security" and the Digital Services Advisory Group and Federal Chief Information Officers Council, "A Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs."

accounts in accordance with organization-defined procedures or conditions; and (4) specifying the required controls for the use of external information systems, such as personal devices, that may process, store, or transmit organization-controlled information on behalf of the organization.

While USAID did not previously terminate user sessions automatically, OCIO officials set up a session control during the course of our audit that automatically requires reauthentication every 7 days within the external cloud system regardless of how the user accessed it. However, according to NIST SP 800-46, requiring reauthentication every 8 hours is considered a best practice. The external cloud system allows the system administrators to specify the duration of the web session to 1 hour, 4 hours, 8 hours, 12 hours, 20 hours, 24 hours, 7 days, 14 days, 30 days, or "session never expires." USAID opted for the 7-day setting because, according to OCIO officials, anything shorter than a week would inconvenience users.

USAID also did not implement controls to automatically lock external cloud system sessions after a period of inactivity when accessed directly from a personal network outside of the secure remote access site. Agency officials acknowledged and OIG confirmed that the external cloud system did not automatically terminate user sessions after 60 minutes of inactivity, as required by the Agency.

Therefore, once users logged into the external cloud system, they remained connected until they manually logged off or were automatically logged off after 7 days, greatly increasing the risk to USAID's information if unauthorized users gain physical access to staff's personal devices.

Further, USAID did not always identify or cancel external cloud system user accounts for personal services contractors (PSCs) when the accounts were no longer required. This could result in contractors having unauthorized access to USAID information and systems, including email, and misusing Government systems or information. For example, one contractor who left and later returned found that his account had not been deactivated for the 45 days he was gone. Another contractor left and did not return, but still had an enabled account and was logging in 5 months after his departure date. This scenario highlights gaps in USAID's process of monitoring and deactivating accounts after 90 days of inactivity.

Finally, USAID did not require security controls on personal devices, such as password protecting devices or updating the operating system to the latest version. As a result, USAID did not have assurance that its information was protected when staff accessed its systems with personal devices.

Roles and responsibilities

Controls over roles and responsibilities include defining the part that each individual plays in a particular operation or process, and the specific tasks or duties that they are expected to complete as a function of their roles, known as privileges.

USAID policies and procedures did not define privileges for external cloud system administrator roles.[11] While USAID had 10 Agency-created administrator roles to meet specific needs and a description of each role, it had not documented the privileges for those roles. For example, USAID had one Agency-created administrator role called "user account operations" that had been given 30 individual privileges in the system, such as adding a new user. However, USAID had not documented the privileges that should have been assigned to this system administrator role, so there was no assurance that the role needed all 30 privileges. Although USAID officials stated that they periodically review roles, the Agency was still at risk that system administrators had inappropriate access that was not commensurate with their responsibilities.

Ethics and legal concerns

Controls that address ethics and legal concerns include confiscation rights and liability issues. USAID policies did not fully address conditions that may require an individual's personal device to be confiscated. Specifically, the Automated Directives System (ADS) states that "individuals must not process, download, or transfer classified data (Confidential [C], Secret [S], or Top Secret [TS]) to unclassified systems or their personal devices."[12] In addition, it warns that in the event of a spillage incident, USAID officials may review the individual's personal electronic device, which may result in wiping stored data and software—up to and including completely wiping or physically destroying the personal device in cases of classified spillage. However, USAID policies did not fully address other conditions that may require personal devices to be confiscated for computer forensics, such as when individuals use their personal devices to gain unauthorized access or when an individual downloads or transfers sensitive but unclassified information on a personal device. Given these incomplete policies, the Agency was at risk of not always having the authority to confiscate and review an individual's device when needed.

Asset management and privacy

Controls over asset management and privacy include (1) reporting and tracking lost or stolen personal devices used for work, (2) removing all Government information if a personal device used for work is lost, stolen, or sold, or if employment is terminated, and (3) documenting a process for employees to safeguard private information if the Government must wipe the device.

USAID policies did not require the reporting and tracking of lost or stolen personal devices that were used to access the external cloud system. If a staff member's device was lost or stolen, an unauthorized individual could have access to Agency resources for up to 7 days. In addition, USAID policies did not require the Agency to wipe its information from a personal device once it was reported as lost or stolen. As a result, if

[11] A system administrator manages a computer system, including its operating system and applications, and normally has special privileges, such as access to security settings. While most of the external cloud system administrators were OCIO staff, some were located in the Office of U.S. Foreign Disaster Assistance.

[12] ADS chapter 552, "Cyber Security for National Security Information (NSI) Systems," May 9, 2018.

a staff member no longer had the personal device that contained sensitive Agency information, USAID officials did not have the authority or ability to wipe the information from the device.

In addition, USAID policies did not have a process for staff to safeguard their personal information if USAID wiped their personal devices. According to NIST SP 800-46, agencies benefit when allowing staff to use personal devices by saving on equipment costs since they do not have to issue devices to all staff. However, staff should be aware of the security incidents that may require all information to be wiped from their personal devices. The potential of losing personal information could create a stressful situation for staff and discourage them from using their personal devices. As a result, the Agency may not reap the potential benefits of having a remote workforce, such as cost savings and lower staff absenteeism.

Devices and applications

Controls over devices and applications include (1) identifying permitted and supported devices to prevent the introduction of malicious hardware and firmware, and (2) defining applications that are required, allowed, or banned.

USAID's policies did not identify permitted and supported devices to prevent the introduction of malicious hardware and firmware when staff accessed the external cloud system without going through the Agency's secure site. For example, based on communication with USAID OCIO officials, Android devices were not allowed because they were not as secure as Apple devices. However, after OIG logged in with an Android device, OCIO officials confirmed that the Android devices could still connect to the usaid.gov external cloud system domain—both through the secure remote access site and outside it. OCIO officials did not believe there was a specific policy denying Android devices from connecting to the external cloud system.

In addition, USAID OCIO officials did not have a list of required, approved, or disapproved applications. Therefore, staff could use applications, such as screen recorders, that put the Agency's sensitive information at risk. OCIO officials stated that, although there was no defined list of approved or disapproved applications, a policy was in draft.

SEVERAL FACTORS PREVENTED FULL IMPLEMENTATION OF KEY CONTROLS FOR PROTECTING INFORMATION ACCESSED ON PERSONAL DEVICES

We identified four reasons why USAID did not fully implement the key controls for protecting information accessed on personal devices. Namely, USAID did not (1) establish clear policies and procedures for staff's use of the external cloud system, (2) conduct a risk assessment, (3) enact safeguards to prevent users from improperly

accessing the system, and (4) manage contractors' access to Agency systems. As a result of these weaknesses, USAID was at risk that its staff were not securely accessing their USAID external cloud system accounts on personal devices.

USAID Did Not Have Clear Policies To Restrict or Provide Procedures on How Staff Should Use Their Personal Devices To Access Agency Information and Systems

USAID policies on the acceptable use of personal devices were confusing. Agency policy stated that users "must not store USAID sensitive information on personal equipment" and "must not send and/or store USAID sensitive information to a personal e-mail account."[13] This implies that personal devices can be used for USAID information that is not sensitive but unclassified. Moreover, USAID policy stated that "RSA Remote Access Soft Tokens can be used on USAID employees' and contractors' personally owned mobile smart devices."[14] However, this policy did not require or restrict access to USAID systems via the Agency's secure remote access site or by using Government-furnished equipment only. (Refer to the Introduction on pages 1-2 for an explanation of the two different login methods for the external cloud system.) Therefore, the policy seemed to allow access to USAID's network and information systems outside the secure remote access site and on personal devices.

In addition, the policy stated that users must not connect non-USAID-issued mobile computing devices, including storage devices, to the USAID network or information systems. This appeared to restrict the use of personal devices, though it was unclear whether this restriction applied to remote access.

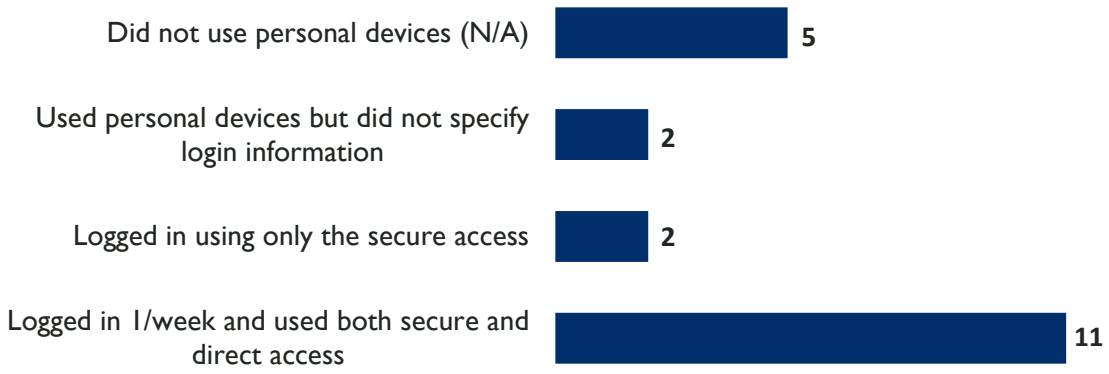
After informing USAID officials of the confusing policies, we were provided a draft revision of the Mandatory Reference for ADS chapter 545, "Rules of Behavior for Users."[15] The revision would restrict users to only access USAID systems on personal devices via the secure remote access site. Once USAID issues this revised rules of behavior and consistently includes this language in all other related policies, the Agency will have clearer restrictions for accessing the external cloud system on personal devices.

Clear Agency-wide communications and ongoing training are critical to ensuring that USAID's requirements and restrictions are implemented as intended, especially since staff were accessing the external cloud system outside of the secure remote access site. For example, of 20 surveyed staff, 11 logged into their USAID external cloud system account at least once per week using personal devices and stated that they used both the secure remote access site and direct access through the public Internet (figure 2).[16]

[13] USAID, "Rules of Behavior for Users: A Mandatory Reference for ADS Chapter 545," August 1, 2013.
[14] USAID, Mandatory Reference for ADS Chapter 545, "Guidelines for Remote Access Soft Tokens for Personal Devices," November 9, 2012.
[15] As of the Exit Conference on October 4, 2019, the draft revision was still not issued.
[16] As of August 30, 2017, USAID had 12,938 active users in the external cloud system.

Of the 15 who responded as personal device users, only 2 staff members said that they always used the secure remote access site to log into their USAID external cloud system account on their personal devices.

Figure 2. Surveyed Staff's Use of Secure Remote Access Site vs. Direct Access



Sample size n=20
Source: OIG, based on results of staff survey

USAID Did Not Perform a Risk Assessment on the Use of Personal Devices for Remote Access to USAID Information and Systems

Performing a risk assessment on the use of personal devices for remote access to USAID resources is critical for identifying risks that require controls, such as the risk of staff downloading sensitive Agency information to personal devices. USAID officials stated that they did not perform a risk assessment, because Agency business should be done using Government-furnished equipment, not personal devices. Although not reflected in policy, officials later confirmed that staff were permitted to use personal devices when logging into the secure remote access site. Without a risk assessment, the Agency did not identify the policies and procedures needed to mitigate the risks of using personal devices.

USAID Did Not Implement Automated Protection To Prevent Staff From Logging Directly Into Their Agency Accounts on Personal Devices

Users had the ability to connect their personal devices to USAID's external cloud system without going through the Agency's secure remote access site. (Refer to the Introduction on pages 1-2 for an explanation of the two different login methods for the external cloud system.) USAID officials explained that, given the way that the secure remote site functions, any controls placed on RSA tokens would restrict logging into the USAID network remotely—whether through the external cloud system's public website or the Agency's secure site. According to USAID officials, personal devices were

allowed but only through the secure remote access site, as it would be cost prohibitive to issue Government laptops to all staff for remote access; however, this restriction was not reflected in policy.

USAID Did Not Have Effective Procedures and Consistent Policies for Notifying Network Administrators When Contractors No Longer Needed Access to Agency Systems, Including the External Cloud System

USAID utilizes PSCs and institutional support contractors. PSCs largely function as Agency employees while institutional support contractors, by contrast, fill a more external role in supporting Agency operations and augmenting the Agency's direct hire and personal services staff.

Personal services contractor accounts

USAID policy states that an Agency supervisor is responsible for managing PSCs.[17] This role includes notifying network administrators when a PSC's network account is no longer needed. OCIO staff have the capability to set up contractor accounts with an expiration date to match the contract end-date, but this was not a required procedure, and no one was actively tracking or reviewing contractor accounts. Further, if no request is submitted to cancel an account or if the request is not submitted in a timely manner, PSCs will have system access beyond their contract end-date. For example, we found that a PSC left the Agency and did not return but still had an enabled account and was logging in 5 months after his departure date. During the course of our audit, OCIO implemented a procedure to automatically disable accounts after 90 days of inactivity.[18] However, that would not have disabled the PSC's account because the individual had been continuing to log in. Therefore, if a request to terminate access is not submitted in a timely manner or at all, a contractor who continues to log in will have system access beyond their contract end-date.

Institutional support contractor accounts

Rather than reporting to a USAID supervisor, institutional support contractors report to the contracting officer or contracting officer's representative (COR) overseeing their contract. USAID did not maintain a record of institutional support contractors who left the Agency and did not have a centralized process for monitoring whether their accounts were properly deactivated in a timely manner. According to OCIO officials, contracting officials, administrative management staff, system managers, and mission executive officers were responsible for notifying OCIO officials when staff no longer needed access to the USAID network, including the external cloud system. USAID's Office of Management Policy, Budget and Performance issued a policy for COR oversight of institutional support contractors, which included a requirement for

[17] ADS chapter 309, "Personal Services Contracts With Individuals," September 20, 2019.
[18] Operation and Maintenance of USAID's Information Technology Infrastructure and Systems Program, "Inactive Account Review Verification Process," February 8, 2018.

notifying OCIO officials when employees no longer needed access to the USAID network. However, OCIO's policy did not include this requirement.

During the course of our audit, OCIO provided a draft revision of the Mandatory Reference for ADS chapter 545, "Rules of Behavior for Users," stating that users must "immediately notify the System Owner or Administrative Management Staff/Executive Management Team … when there is a change in [their] employee status and/or access to an IT system is no longer required." However, this draft language did not explicitly include contracting officers or CORs who are responsible for overseeing the institutional support contractors.

CONCLUSION

While OCIO officials implemented some controls to protect information accessed on personal devices and took action to address some weaknesses we identified during our audit, significant gaps remain in the Agency's policies on the use of personal devices. Those gaps present an increased risk of a breach of USAID's external system and the information in it. Until OCIO assesses the risks and establishes clear policies and procedures on the proper use of personal devices, the Agency will continue to lack assurance that its information and the external cloud system are secure.

RECOMMENDATIONS

We recommend that USAID's Chief Information Officer:

1. Conduct a risk assessment of the current session termination setting of 7 days versus the 8-hour best practice for the external cloud system, and take the necessary action based on the results of the risk assessment.
2. Develop and implement written policies and procedures for Agency-created external cloud system administrators to clearly define and specify the privileges that should be assigned to each role.
3. Conduct a risk assessment for Agency staff using personal devices to access the external cloud system and determine what actions Agency officials need to take to mitigate any identified risks. This includes updating relevant policies to consistently reflect the acceptable use of personal devices as deemed appropriate by management and providing training to staff on those new policies.
4. Develop and implement policies and procedures to promptly disable network accounts for contractors when the contracted work ends.

OIG RESPONSE TO AGENCY COMMENTS

We provided our draft report to USAID on April 8, 2020, and on May 26, 2020, received its response, which is included as appendix B.

The report included four recommendations. We consider three of them closed (recommendations 1, 2, and 4), and one resolved but open pending completion of planned activities (recommendation 3).

We acknowledge management decisions on all four recommendations.

APPENDIX A. SCOPE AND METHODOLOGY

We conducted our work from June 2017 through April 2020 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.

Our audit objective was to determine whether USAID implemented key internal controls to protect information available in the external cloud system when accessed through staff's personal devices based on controls recommended by the National Institute of Standards and Technology, Digital Services Advisory Group, and Federal Chief Information Officers Council. Specifically, we assessed (1) USAID's implementation of key internal controls related to access, identification and authentication, system and communications protection, roles and responsibilities, education, privacy, ethics and legal concerns, devices and applications, and asset management and (2) factors that may have affected USAID's implementation of these controls.

The audit was initiated after OIG became aware that Agency staff could access their USAID external cloud system accounts directly on their personal devices outside of the secure remote access site, which presented a security concern. To develop the objective, we researched and nonstatistically selected key security controls that we believed represented the highest risks to the use of personal devices for remote access. Specifically, we identified key security controls in:

- The National Institute of Standards and Technology Special Publication 800-46, "Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security." We reviewed controls within 3 of 6 security control categories:
    - Access controls, including account management, session lock and termination, Agency requirements for personal devices, and use of external information systems.
    - Identification and authentication, including periodic reauthentication.
    - System and communications protection, including transmission confidentiality and integrity.
- The Digital Services Advisory Group and Federal Chief Information Officers Council's "A Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs." We reviewed controls within 6 of 10 security control categories:
    - Roles and responsibilities of system administrators and users.
    - Education, including trainings and user agreements.
    - Privacy, including personal versus organizational security and safeguarding personal information.

- Ethics and legal concerns, including defining "acceptable use" of personal devices and confiscation rights.
- Devices and applications, including identifying required, allowed, and banned applications; permitted and supported devices; content storage in cloud versus personal devices; and ownership of the information.
- Asset management, including wiping information on lost or stolen personal devices, and reporting and tracking lost or stolen personal devices.

Due to the nonstatistical nature of our sample, our results cannot be projected to the entirety of the Agency's remote access control environment.

The period under audit was fiscal year 2017 through fiscal year 2019, and the fieldwork took place in Washington, DC.[19]

To answer the objective, we reviewed USAID's policies, procedures, the external cloud system service contract, and related documentation to identify the selected internal controls, which would reduce the risk of compromised Agency information when the external cloud system is accessed on personal devices. In addition, we conducted tests to review the selected controls. When we found inconsistencies, we brought them to USAID OCIO officials' attention.

Specifically, we reviewed USAID's service contract files to identify USAID's responsibilities for controls over the applications versus the responsibilities of the vendor. Also, we reviewed USAID policies, procedures, and other documents such as:

- ADS chapter 545, "Information Systems Security"
- Mandatory reference for ADS chapter 545, "Rules of Behavior for Users"
- ADS chapter 552, "Cyber Security for National Security Information Systems"
- "Mobile Security Guidance"
- "Mobile Device Lock/Wipe Policy and Procedures"
- "Inactive Account Review Verification Process"
- RSA SecurID Software Token guides
- USAID Remote Token Agreement Form
- Authority to operate the external cloud system
- "Plan of Action and Milestones Detail Report for [the external cloud system]"
- Security plan for the external cloud system

In fiscal year 2017, we tested the inactivity time-out and automatic session termination controls on a personal device directly through the external cloud system's public

[19] Given the internal control nature of the audit objective, we reviewed controls in place at the time of initiation in fiscal year 2017. However, this audit incurred many delays as a result of competing priorities. Therefore, the period under audit was longer than intended and ended in fiscal year 2019.

website. In fiscal year 2019, after Agency notification that a 7-day automatic session termination control was recently implemented, we retested those external cloud system controls on a personal device.

We also reviewed the status of the external cloud system accounts for a nonstatistical sample of staff that separated from July 1 to October 28, 2017. The Office of Human Capital and Talent Management provided a list with a universe of 215 separated staff for this period. Using nonstatistical sampling, we reviewed approximately 10 percent of the 215 staff—or 22 individuals. We believed 10 percent was sufficient to conclude whether the list accurately reported staff who had left the Agency. In order to select the users, we selected every 10th name on the list, which was sorted by departure date. We eliminated USAID OIG staff from our selection and replaced them with the previous name on the list. To finish our review, on November 30, 2017, we went through the selected users to monitor their account status in the external cloud system. Specifically, we checked whether the accounts were disabled and when they last logged in. Due to the nonstatistical nature of our sample, our testing results cannot be projected to the entirety of separated staff.

We surveyed a nonstatistical sample of USAID's 12,938 active users in the external cloud system to assess their use of the application in fiscal year 2018.[20] Our sample of 20 was sufficient for us to gain an understanding of how staff were accessing the system on their personal devices. For this review, we wanted to select both Washington and overseas staff, because there may have been differences in how they used their devices. Therefore, we selected 15 Washington staff and 5 El Salvador staff. We selected El Salvador because it had a similar time zone to our team, which would make it easier to follow up with the staff. We sent out a survey in January 2018 asking for responses to questions on the following: (1) use of personal devices to access USAID's external cloud system, (2) if they stayed logged into the external cloud system, (3) if they usually logged into the external cloud system at least once per week, (4) if they had personal devices that did not have a password, passcode, or biometric (e.g., fingerprint) enabled to unlock them, (5) if they had personal devices that were used for work without time-out or auto-lock enabled, (6) if they had any security applications on their personal devices, and (7) if they were aware of any controls that prevented them from sending personally identifiable information or sensitive but unclassified information to recipients outside the Agency when using the external cloud system on their personal devices.

After analyzing the responses, in May 2018, we sent a followup message asking an additional question to the 15 staff who had confirmed in our initial survey that they used personal devices to access the external cloud system. We obtained a response to the additional question from 13 of the 15 staff members; one had retired and the other was out of the office for an extended period of time. We analyzed the 13 responses to determine how the staff logged into the external cloud system on their personal devices

[20] This universe of 12,938 active users was generated by USAID's external cloud system on August 30, 2017.

(i.e., via the secure remote site, directly on the external cloud system's public website, or both). Due to the nonstatistical nature of our sample, our testing results were not projected to the entirety of the external cloud system users.

We also conducted interviews with Agency officials in OCIO, including the chief information officer, the contracting officer's representative for the external cloud system service contract, and the external cloud system primary administrator. We vetted our conclusions with OCIO officials and updated our findings as necessary based on changes to controls, policies, and procedures.

Regarding data reliability, we verified the accuracy of the separated staff list that the Agency provided but did not rely on the raw data for our conclusions. Also, for the accuracy of the user account information in the external cloud system, we reviewed the Security Assessment Report for the external cloud system, which was completed by an independent third party and recommended that a continued FedRAMP authorization be granted for the external cloud system. This recommendation was based on the risks identified and the continuous improvement of security-related processes and controls. Lastly, we found that none of the risks identified in the Security Assessment Report had a concern or issue with the integrity of the external cloud system accounts.

To further assess data reliability, we evaluated the reasonableness of the number of system administrators for the external cloud system in fiscal year 2017. For the review, we met with OCIO staff to obtain information on system administrators, their account status and assigned privileges. We took screenshots from the system to determine the total number of active USAID external cloud system user accounts; the list of different types of administrator roles that USAID had and used, including a description for each administrator role type and the privileges assigned to each role; and the total number of staff assigned to each of the different administrator roles. For each of these roles, we calculated the ratio of administrator-to-regular-user by using the following formula: (Total Active Users - Total Administrators for Role) divided by the Total Administrators for Role.

We asserted that a reasonable number of system administrators for each role was no more than 2 percent of the active 12,938 users. We also looked at the office or location of each administrator to quantify how many were overseas versus U.S.-based. Lastly, we checked whether any of the assigned administrators were in the Office of Human Capital and Talent Management's separated staff list to ensure none had left the Agency and still had an active account. We determined that the data were sufficiently reliable for the purposes of our report.

APPENDIX B. AGENCY COMMENTS

MEMORANDUM

TO: Deputy Assistant Inspector General for Audit, Alvin Brown

FROM: Assistant Administrator for the Bureau for Management, Frederick M. Nutt /s/

DATE: May 22, 2020

SUBJECT: Management Comments to Respond to a Draft Audit Report Produced by the Office of the Inspector General (OIG) Titled, *USAID Needs To Improve Policy and Processes To Better Protect Information Accessed on Personal Devices* (A-000-20-00X-P)

The U.S. Agency for International Development (USAID) would like to thank the Office of the Inspector General (OIG) for the opportunity to provide comments on the subject draft report. The Agency agrees with the recommendations, herein provides plans to implement them, and reports on significant progress already made.

The Agency's Chief Information Officer (CIO) believes we have addressed three of the report's four recommendations to improve USAID's control environment to protect information available in our external cloud system when our staff connect to it through their personal devices. The fulfilment of the remaining open recommendation is pending the Agency's implementation of a technical Cloud-Access Security Brokers solution, which will prevent our employees or contractors from using any personal device to gain direct access to our data. The Office of the CIO within the Bureau for Management anticipates having this security feature in place by March 2021, unless exigencies caused by COVID-19 create a delay.

COMMENTS BY THE U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT (USAID) ON THE REPORT RELEASED BY THE USAID OFFICE OF THE INSPECTOR GENERAL (OIG) TITLED, *USAID Needs To Improve Policy and Processes To Better Protect Information Accessed on Personal Devices* (A-000-20-00X-P) (Task No. AA100617)

Please find below the Management Comments from the U.S. Agency for International Development (USAID) on draft report A-000-20-00X-P produced by the Office of the USAID Inspector General (OIG), which contains four recommendations for USAID:

Recommendation 1: Conduct a risk-assessment of the current session-termination setting of seven days versus the eight-hour best practice for the [Agency's] external cloud system, and take the necessary action based on the results of the risk-assessment.

- **Management Comments:** USAID agrees with this recommendation, and we believe the Agency has taken sufficient action to address it. On November 7, 2019, our Chief Information Officer (CIO) signed a risk-acceptance memorandum (Tab B) to change the seven-day session timeout to 24 hours. Having a session timeout every eight hours would make our external cloud systems and services less available, and would create undue inconvenience and stress for our users. Our CIO has determined the 24-hour maximum for a session strikes a good balance between security and our operational business and communications requirements. We have re-configured our external cloud system to enforce this 24-hour timeout.

- **Target Completion Date:** USAID requests the OIG to close this recommendation upon issuing the final report.

Recommendation 2: Develop and implement written policies and procedures for Agency-created external cloud-system administrators to clearly define and specify the privileges that should be assigned to each role.

- **Management Comments:** USAID agrees with this recommendation, and we believe the Agency has taken sufficient action to address it. Our CIO has documented the Access-Control Procedures for the provider of our external cloud system (Tab C), to ensure the confidentiality, integrity, and availability of our information-technology (IT) systems and our data. Section 2.1 of the Access-Control Procedures specifies each administrative role assigned within the system and the privileges associated with it.

- **Target Completion Date:** USAID requests the OIG to close this recommendation upon issuing the final report.

Recommendation 3: Conduct a risk-assessment for Agency staff using personal devices to access the external cloud system and determine what actions Agency officials need to take to mitigate any identified risks. This includes updating relevant policies to reflect the acceptable use of personal devices consistently as deemed appropriate by management and providing training to staff on those new policies.

- **Management Comments:** USAID agrees with the recommendation. However, in lieu of conducting a risk-assessment for Agency staff who are using personal devices to connect to our cloud systems, our approach to addressing this recommendation will be to implement a Cloud Access Security Broker (CASB) solution that will prevent our employees or contractors from using any non-Government-Furnished Equipment (GFE) to gain direct access to USAID's data. Through configuration, the solution will require all access to cloud services to go through CASB. CASB uses a USAID-issued Non-Person Entity (NPE) certificate to distinguish GFE (Windows, MacBook, iPhone, iPad devices) from non-GFE Devices. We therefore would restrict our cloud services to GFE and strictly enforce this policy.

- **Target Completion Date:** March 31, 2021.

Recommendation 4: Develop and implement policies and procedures to disable network accounts promptly for contractors when the contracted work ends.

- **Management Comments:** USAID agrees with the recommendation, and we believe the Agency has taken sufficient action to address it. On April 10, 2020, the Office of Acquisition and Assistance within the Bureau for Management (M) implemented revised Chapter 302 of the Agency's Automated Directives System (ADS) (Tab D), USAID Direct Contracting. This Chapter describes our policy directives, required procedures, and internal guidance for the procurement of goods and services through direct contracts for the purposes of implementing our activities and supporting our logistics. ADS Chapter 302.3.5.13, Access to USAID Facilities and USAID's Information Systems, establishes the requirement for Contracting Officer's Representatives (CORs) to revoke access to the Agency's IT systems for contractors upon the termination of their contracts. In addition, a mandatory reference to updated ADS Chapter 306mah, *Contracting Officer Representative (COR) Checklist: Exit Procedures for Institutional Support Contractors and Federal Employees Under Interagency Agreements* (Tab E), describes the checklist every COR must complete for the following circumstances:

    - The signature of an institutional support contract and the termination of the employment of individual contractors under such a contract; and
    - The signature of an interagency agreement (IAA) and the termination of the employment of a U.S. Direct-Hire Federal employee under an IAA.

According to the checklist, when a contractor's employment ends, the cognizant COR must transmit an affirmative notification to the relevant Executive or Administrative Management Support (AMS) Officer, who works with the Office of the CIO within the M Bureau to disable the contractor's access to the Agency's IT systems.

- **Target Completion Date:** USAID requests the OIG to close this recommendation upon issuing the final report.

In view of the above, we request that the OIG inform USAID when it agrees or disagrees with a Management Comment.