MEMORANDUM

DATE: December 22, 2020

TO: USAID, Chief Financial Officer, Reginald W. Mitchell

FROM: Deputy Assistant Inspector General for Audit, Alvin A. Brown /s/

SUBJECT: Transmittal of Management Letters for USAID's Fiscal Year 2020-2019 Financial Statement Audit Report (0-000-21-001-C)

On November 16, 2020, we transmitted the financial statement audit report performed by the independent public accounting firm of GKA P.C. (GKA). The auditors issued an unmodified opinion on USAID's fiscal year (FY) 2020-2019 financial statements.

When performing an audit of an agency's financial statements, auditors may identify certain matters involving internal controls that do not rise to a level of significance to be reported in the independent auditors' opinion report; instead these matters are communicated in a management letter. We have attached to this memorandum a copy of the two FY 2020-2019 management letters dated November 23, 2020, which report on such matters.

These letters do not affect the auditors' unmodified opinion on the financial statements. GKA is responsible for the enclosed letters and the conclusions expressed in them.

We appreciate the assistance provided to our staff and the audit firm's employees during the engagement.

gka, p.c.
Certified Public Accountants
& Consultants

1920 L Street, NW, Suite 425
Washington, DC 20036
Tel: 202-857-1777
www.gkacpa.com

U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT

MANAGEMENT LETTER
FISCAL YEAR 2020

November 23, 2020

Chief Financial Officer and Inspector General
U.S. Agency for International Development
Washington, D.C.

We have audited the consolidated financial statements of U.S. Agency for International Development (USAID), which comprise the consolidated balance sheet as of September 30, 2020 and 2019 and the related consolidated statement of net cost, consolidated statement of changes in net position, and combined statement of budgetary resources for the year then ended, and the related notes to the financial statements (hereinafter referred to as the "consolidated financial statements"), and have issued an unmodified opinion thereon dated November 9, 2020. In planning and performing our audit of the financial statements of USAID, we considered its internal control over financial reporting in order to determine our auditing procedures for the purpose of expressing our opinion on the financial statements and not to provide assurance on the internal control. We have not considered the internal control since the date of our report.

During our audit, we noted certain matters involving the internal control over financial reporting, compliance and other operational matters that are presented in this letter for your consideration. The comments have been discussed with the appropriate members of USAID Management, are intended to improve the internal control over financial reporting or result in other operational efficiencies.

We appreciate the cooperation and courtesies extended to us. We will be pleased to meet with you or your staff at your convenience to furnish any additional information.

/s/

November 23, 2020

1. *The process for identifying and investigating potential funds controls violations needs to be strengthened. (Repeat)*

We noted that seven Letter of Credit (LOC) grantees had instances of advances or liquidations for expenditures which exceeded the amount authorized by approximately $1.2 million.

Automated Directive Systems (ADS) chapter 634.3.5.1 paragraph a.5, states that: *Congress enacted the Anti-deficiency Act (ADA) to prevent the obligation of government funds that are not available. Violations of the ADA can occur when an officer or employee authorizes or creates an obligation or makes expenditure in excess of an apportionment or reapportionment. This includes adjustments that cause obligations in expired accounts to exceed the apportionment for the year in which such obligations were incurred.*

ADS 634, requires that USAID *"Establishes, maintains, and oversees the Agency's system of funds control in accordance with Federal law and OMB guidance."* To that end, the Bureau for Management's Chief Financial Officer (M/CFO) has the responsibility to investigate and determine whether funds control violations did occur, and to classify the violations as either administrative funds control violations or violations of ADA. Violations of ADA require the CFO to immediately inform the Office of the Inspector General and the Congress of the United States.

The lack of prompt review of potential funds control violations increases the risk that an Anti-Deficiency Act violation may occur and not be detected.

2. *The process for identifying and liquidating outstanding advances for Non-Letter of Credits (NLCs) should be strengthened. (Repeat)*

The Agency continues to have unliquidated advances outstanding for more than 150 days (*See "Table 1" below*). In addition, the balance for NLC has decreased in FY20 by $135 million (22%); however, the NLC advances outstanding greater than 150 days continues to grow from year to year (with the exception of FY17). The most significant change occurred from FY18 to FY19. The balance grew by $190 million (44%) between FY2018 and FY2019; by approximately $80 million (23%) between FY2017 and FY2018; and by approximately $20 million (6%) between FY2015 and FY2016. This indicates that advances are not being liquidated promptly. The table below details advances that were outstanding as of the end of the fiscal years noted, along with the dollar and percentage increase/(decrease) from year to year.

Table 1: Analysis of Aging of Advances and Balances Per FYs

Fiscal Year	Total Advances	$ Change	% Change	Advances Older than 150 Days	$ Change	% Change
FY20	$484,765,772	$(135,221,634)	(21.81%)	$55,848,070	$2,278,728	4.25%
FY19	619,987,406	190,084,237	44.22%	53,569,342	13,656,815	34.22%
FY18	429,903,169	79,730,849	22.77%	39,912,527	3,491,278	9.59%
FY17	350,172,320	(6,206,371)	(1.74%)	36,421,249	(6,671,781)	(15.48%)
FY16	356,378,692	19,837,518	5.89%	43,093,030	6,288,074	17.08%

NLCs are composed of advances to US Governmental Agencies (e.g.: State Department) and to non-governmental entities (e.g.: U.N., World Bank). The Agency's position is that the Agency uses its discretion to determine whether to advance funds in excess to three months. Furthermore, the Agency assumes that advances to other US Government Agencies create no risk advances because they are between inter-related entities. However, most of these advances are old. As of September 30, 2020, $19 million out of $23 million of the total government advances (84%) represented advances older than 150 days. In addition, the balances of advances that are growing the fastest (at a rate of 34%) are those to non-US Government entities.

Statement of Federal Financial Accounting Standards No. 1, "Accounting for Selected Assets and Liabilities," paragraph 59, states that: *Advances and prepayments are reduced when goods or services are received, contract terms are met, progress is made under a contract, or prepaid expenses expire.*

According to USAID's ADS 636, USAID Mission Controllers and the Agency's Cash Management and Payments Division must ensure that requests for the advance of funds are reasonable and not excessive to the recipients immediate disbursement needs. Funds in excess of immediate disbursement needs shall be refunded to the Agency. The only exceptions are when the excess funds will be disbursed within seven (7) days or when the amount is less than $10,000 and will be disbursed within thirty (30) days.

On September 19, 2014, the Agency implemented a policy extending the reporting period to 120 days and the period advances can be outstanding before being declared delinquent from 90 days to 150 days. Specifically, the policy states that: *Generally, advance payments or any portion of an advance payment not liquidated within 150 days (120 days for voucher submission plus 30 days for processing) is considered delinquent. A documented rationale from the Agreeing Officer (AO)/ Agreement Officer Representative (AOR) and approved by the Controller for Missions, or Chief of M/CFO/CMP for Washington, must support any exception.* (See ADS Reference 636MAA pg. 4 par. 2- https://www.usaid.gov/ads/policy/600/636maa)

This policy allows the Agency to not report as late advances older than 90 days because it assumes that (a) grantees will take 30 days to report the expenses, and (b) the Agency will take another 30 days to liquidate the advances. As a result, advances are outstanding for 150 days or more before they are even considered for liquidation; and advances between 90 days and 150 days old are not considered late and subject to liquidation.

Liquidations are not being applied promptly and balances in the NLCs are accumulating. Failure to liquidate advances within the approved timelines increase the risk that the balance of advances in the financial statements may not be accurate, since these amounts may have already been spent and should no longer be presented as advances.

3. *Intragovernmental Transactions Remain Unreconciled (Repeat Finding-Modified)*

When a Federal Government Agency buys goods or services from another Agency, the two engage in an intragovernmental transaction and are referred to as "trading partners." Differences arise in Government-wide financial reporting when Agencies record such transactions in different periods or make accounting errors. In FY2013, Treasury developed "scorecards" to track and correct these differences. The scorecards rank each Agency by its contribution to the Government-wide differences.

At the end of FY2019, USAID had unreconciled differences of $463 million, and was ranked the 14th largest contributor out of 140 Agencies. As a result, USAID was required to reconcile, resolve, and confirm the outstanding differences, but has been unable to do so. USAID IGT differences at the end of the third quarter (Q3) of FY 2020 recorded by Treasury was $1.3 billion and the Agency was ranked 13th largest contributor.

The prior year FY 2019 final Treasury Scorecard, issued in FY 2020 reported that the Agency did not meet 2 of the 18 entity performance measurement goals:

1. Governmentwide Treasury Account Symbol Adjusted Trial Balance System (GTAS) Submission – 90% (All Treasury Account System (TAS)) and 100% (expenditure TAS) submitted by 11/14/19.
2. Legal Representation Letter/Legal Letter/Management Schedule Template:

   i. Interim due 8/22/2019.
   ii. Final due 11/19/2019 Excel Format per Treasury Financial Manual Volume 1, Part 2, Chapter 4700 Section 4706.30a (ITFM 2-4700, Main Chap. 4705.60a).

Also, the Q3 FY 2020 Scorecard suggested three Corrective Actions for the Agency:

- Ensure G-Invoicing Implementation Plans are submitted to Fiscal Service by September 30, 2020.
- Address all intra-departmental differences before year-end reporting is complete.
- Work with the General Fund, State Department, and the Department of Labor (DOL) to reduce IGT differences at year-end.

OMB Circular A-136, "Financial Reporting Requirements," August 27, 2020, states that throughout the fiscal year, entities are required to reconcile and resolve differences between intragovernmental balances and transactions. All differences should be resolved prior to final submission of data for the Financial Report of the United States Government.

Treasury Financial Manual Volume 1, Part 2, Chapter 4700 Section 4706.30a states that Federal entities are expected to work with their respective trading partners to reconcile and resolve intragovernmental differences.

Treasury Financial Manual Volume 1, Part 2, Chapter 4700 Section 9 states that while processing transactions through Intragovernmental Payments and Collections (IPAC), trading partners must follow the business rules to avoid the misstatement of financial balances that occurs when trading partners fail to properly record intragovernmental activity.

Treasury's "Intragovernmental Transactions Guide" suggests that Agencies work together to reconcile any differences and prevent them by eliminating long-term accounting policy differences.

Transactions between USAID and other Federal Agencies are primarily recorded by means of Intra-Governmental Payment and Collection (IPACs) prior to their recording in USAID's general ledger. IPACs operate as the application for the settlement of funds between Federal entities. It is incumbent on USAID to obtain and maintain adequate supporting documentation such as requisitions, invoices etc. as support for the IPAC transactions. This is to ensure that these transactions are completely and accurately recorded in the appropriate general ledger accounts, both at USAID/Washington and at the Missions. During its review of IPAC transactions, we noted that over 50% of USAID IPAC transactions are between USAID/Washington and other Federal Agencies. The rest are between USAID Missions and other Federal Agencies. USAID/Washington obtains and maintains support such as requisitions, invoices for its IPAC transactions. However, some of the Missions do not maintain such support. This may contribute to the unresolved differences with trading partners.

There is a risk of misstatement in the financial statements when trading partners fail to properly record intragovernmental transactions.

We acknowledge that USAID has processes in place to resolve unreconciled differences and has made efforts to do so. Still, a significant unresolved balance remains. A similar finding was reported in previous audits, and we recognize that resolution of these differences will require significant coordination with other Federal Agencies. It is unlikely that USAID can resolve this issue working alone.

4. *USAID interface controls between feeder and receiving systems should be improved.*

During our review of reconciliations of the interface between the one feeder system and the receiving system, USAID's accounting system of record, we noted Discrepancy reports of differences between balances and data in the receiving system and the feeder are not being consistently reconciled. USAID resolves the differences on an Ad hoc basis.

United States Government Accountability Office, Standards for Internal Control in the Federal Government (Green Book), requires that *transactions to be promptly recorded to maintain their relevance and value to management in controlling operations and making decisions. This applies to the entire process or life cycle of a transaction or event from its initiation and authorization through its final classification in summary records. In addition, management designs control activities so that all transactions are completely and accurately recorded.*

The Discrepancy Report Standard Operating Procedure, states that:
"*Shared Responsibilities*

- *Review report monthly for any new discrepancies*
- *After the resolution has been implemented, confirm that discrepancy is not displayed on the next report*
    - *Communicate to other team when item has been resolved*
    - *Communicate to other team for additional review in the event that agreed upon resolution does not successfully remove discrepancy from report*"

USAID does not resolve differences between the feeder and the receiving systems systematically. Rather, it is done on an inconsistent or ad hoc basis.

Failure to reconcile and correct errors in the system interfaces could negatively impact the completeness, accuracy, and validity of transactions and data, and the timeliness of their reporting. In addition, discrepancies arising from lack of complete and accurate migration of clean data may affect the accuracy of the financial statements and related information.

5. *Unliquidated obligations (ULOs) are not consistently identified and de-obligated as excess or unneeded funds. (Repeat)*

During FY 2020, USAID implemented the ULO dashboard and Automated De-obligation tool to help track and de-obligate unliquidated obligations without activity for three years or more. USAID and its Missions also review ULOs annually. Though the implemented controls enhanced the process for tracking and de-obligating ULOs, we noted that the Agency and Missions were not consistently de-obligating excess or unneeded funds. When funds are de-obligated, they are made available in the accounting system for reprogramming. During our audit, we analyzed USAID's Unilateral ULOs and determined that, as of September 30, 2020, USAID had approximately $15.2 million in unliquidated obligations with no disbursements for more than three years. These may be available for de-obligation.

DESCRIPTION	AMT
FY2019 ULO Balance (A)	$ 31,672,048
ULO Resolved During FY2020 (B)	(22,584,144)
New ULO Meeting 3-Year Requirement During FY2020 (C)	6,115,699
FY2020 ULO Balance	$ 15,203,603

Additionally, we tested a sample of June 30, 2020 ULOs without activity for three years or more and noted the following exceptions:

- For 10 of the 45 samples tested, evidence of the 1311 review could not be provided.
- For five of the 45 samples tested, the support provided did not agree to the sampled amount.

Under the provisions of US Code, Title 31 Section 1554: Audit, Control, and Reporting,

"*[a]fter the close of each fiscal year, the head of each Agency shall submit to the President and the Secretary of the Treasury a report regarding the unliquidated obligations, unobligated balances, canceled balances, and adjustments made to appropriation accounts of that Agency during the completed fiscal year… Each report required by this subsection shall… contain a certification by the head of the Agency that the obligated balances in each appropriation account of the Agency reflect proper existing obligations and that expenditures from the account since the preceding review were supported by a proper obligation of funds and otherwise were proper.*" Additionally, the regulation requires that "*[t]he head of each Agency shall establish internal controls to assure that an adequate review of obligated balances is performed.*"

In addition, USAID's Automated Directives System (ADS) Chapter 621, "Obligations," requires USAID and its Missions to initiate and coordinate reviews of all ULOs, at least annually, to determine whether their balances should be retained or deobligated.

These deficiencies occurred because obligation managers did not consistently monitor the performance of the contracts and grants that were assigned to them. Furthermore, the Agency does not require contracting officers to include the period of performance dates in the Global

Acquisition and Assistance System (GLAAS) so that they can be recorded in the accounting system. Finally, the 1311 reviews were not consistently performed and documented.

There is an increased risk of losing program and operating expense funds that may expire before they are de-obligated. Failure to maintain an effective ULO control environment in which invalid open obligations are identified and de-obligated in a timely manner may result in difficulties in managing funds, improper payments, inaccurate budgetary reports, and possible violations of Federal regulations.

6. *Long outstanding reconciling items are not being researched and cleared timely, and Suspense Account items are not being researched and resolved within the Department of the Treasury's 60-day rule (DOWNGRADE from Significant Deficiency to MLC)*

During our review of fiscal year 2020 third quarter Fund Balance With Treasury (FBWT) reconciliation, we reviewed the Treasury GL Reconciliation (TyGR) Analysis performed outside the Electronic Cash Reconciliation Tool (eCART), to determine whether the process was effective. The TyGR process provides a monthly and quarterly summary and detail listing of all outstanding reconciling items by appropriation. Our review of the prior year (fiscal year 2019) TyGR report reconciliation, revealed several long outstanding items that were outstanding for more than the three-month Treasury rule totaling 2,505 and $1.005 billion, in count and absolute values, respectively, which we reported as a significant deficiency.

In fiscal year 2020, our follow-up and review of management actions on the prior year proposed recommendations, revealed the Office of the Chief Financial Officer prepared a Corrective Action Plan (CAP), enforced its policies and procedures and provided resources to identify and clear FBWT reconciling items outstanding for more than the Treasury three-month rule. As a result of the measures implemented by the agency, we noted improvement during the testing of the fiscal year 2020 third quarter FBWT reconciliation. Total long outstanding reconciling items greater than three months decreased by a total of 84% (2,112) and 97% ($970,778,923) in count and absolute dollar amount, respectively, compared with the third quarter of fiscal year 2019. According to the agency, it is on track to clear all long outstanding reconciling items. However, the agency still has aged reconciling items outstanding for more than Treasury three-month rule. The table below illustrates the age, count and absolute amount of outstanding reconciling items at June 30, 2020 (Q3 2020) compared to June 30, 2019 (Q3 2019);

Table 1:

Q3 2020			Q3 2019		Percentage increase/decrease	
Aging Category	**Count**	**Absolute Amount**	**Count**	**Absolute Amount**	**% Count**	**% Absolute Amount**
More than I year	64	$ 10,855,296	690	$ 30,288,587.00	91%	64%
6 - 12 months	103	$ 5,013,000	1058	$ 900,092,477.00	90%	99%
4 - 6 months	81	$ 3,970,128	436	$ 47,328,501.00	81%	92%
91 - 120 Days	145	$ 14,769,360	321	$ 27,677,143.00	55%	47%
Total	**393**	**$ 34,607,784**	**2505**	**$1,005,386,708.00**	84%	97%

During our review of the FBWT Suspense account for the end of the third quarter of fiscal year 2020, we noted the agency prepared a CAP and enforced its policies and procedures to resolve suspense account items within the 60-day timeframe mandated by Treasury. As a result, total suspense account items aged more than the 60-day Treasury mandated timeframe decreased by

63% (1,506) and 30% ($9,207,039) in count and absolute dollar amount, respectively, from the third quarter fiscal year 2019 to the third quarter fiscal year 2020. The agency provided evidence of further decreasing trend at the end of August and year end of fiscal year 2020. However, the agency still has aged suspense items outstanding for more than Treasury sixty-day rule. The table below illustrates the age, count and absolute amount of outstanding suspense account reconciling items at June 30, 2020 (Q3 2020) compared to June 30, 2019 (Q3 2019);

Table 2:

Q3 2020			Q3 2019		Percentage increase/decrease	
Aging Category	**Count**	**Absolute Amount**	**Count**	**Absolute Amount**	**% Count**	**% Absolute Amount**
More than I year	524	$ 3,250,689.00	1553	$ 17,706,836.61	66%	82%
4 - 12 months	282	$ 4,726,121.02	302	$ 2,822,120.07	7%	-67%
2 - 3 months	88	$ 13,510,668.89	545	$ 10,165,560.66	84%	-33%
Total	**894**	**$ 21,487,478.91**	**2400**	**$ 30,694,517.34**	63%	30%

FBWT Reconciliation Procedures, a Supplement to the Treasury Financial Manual, Volume I, part 2-5100, states that federal agencies should not permit prior-month differences to remain outstanding for more than 3 months.

Treasury Financial Manual, Bulletin No. 2017-10 requires that transactions in suspense accounts be cleared within 60 business days of the date of the transaction.

USAID has not completed its fiscal year 2019 corrective action plan commitment to perform timely research and clear **all** outstanding reconciling items within three months and sixty days from the date of transaction, respectively, for reconciling and suspense items, as mandated by the Department of Treasury.

Long outstanding reconciling items represent an area of uncertainty that increases the risk of misstatements in the financial statements. In addition, the longer they remain in suspense, the less likely they are to be resolved.

gka, p.c.
Certified Public Accountants
& Consultants

1920 L Street, NW, Suite 425
Washington, DC 20036
Tel: 202-857-1777
www.gkacpa.com

U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT

MANAGEMENT REPORT
INFORMATION TECHNOLOGY

FISCAL YEAR 2020

November 23, 2020

gka, p.c.
Certified Public Accountants
& Consultants
Member of the American Institute of Certified Public Accountants

Chief Financial Officer and Inspector General
U.S. Agency for International Development
Washington, D.C.

We have audited the consolidated financial statements of U.S. Agency for International Development (USAID), which comprise the consolidated balance sheet as of September 30, 2020 and 2019 and the related consolidated statement of net cost, consolidated statement of changes in net position, and combined statement of budgetary resources for the year then ended, and the related notes to the financial statements (hereinafter referred to as "consolidated financial statements"), and have issued an unmodified opinion thereon dated November 9, 2020. In planning and performing our audit of the financial statements of USAID, we considered its internal control over financial reporting in order to determine our auditing procedures for the purpose of expressing our opinion on the financial statements and not to provide assurance on the internal control. We have not considered the internal control since the date of our report.

During our audit, we noted certain matters involving USAID's information technology (IT) general controls and other operational matters that are presented in this letter for your consideration. We identified three findings related to security management and access controls. The purpose of this report is to provide specific details regarding the findings. The findings have been discussed with the appropriate members of USAID Management and are intended to improve USAID's information technology general controls or result in other operational efficiencies.

We appreciate the cooperation and courtesies extended to us. We will be pleased to meet with you or your staff at your convenience to furnish any additional information.

/s/

November 23, 2020

Improvements Needed in Information Technology (IT) General Controls over USAID's Financial Systems

During our audit, we identified three findings related to IT security management and access controls that are discussed below.

(A) Security Management

An entity wide information security management program is the foundation of a security control structure and a reflection of senior management's commitment to addressing security risks. During our audit, we noted one finding in this area.

1. Controls over the monitoring of external service providers for one system should be strengthened

We noted that:

- The Service Level Agreement (SLA) between USAID and the Department of State (DoS) for one system's hosting service has not been reviewed and updated since it was signed by the former CFO on October 31, 2013. The current CFO was hired in 2014. The SLA, which requires annual reviews, has not been updated to reflect this change.

ADS Chapter 545.3.2.14, Use of External *Information Systems,* states that:

- System Owners (SO) must establish terms and conditions consistent with any trust relationships established with other organizations owning, operating, or maintaining external information systems. The terms and conditions must include provisions for allowing authorized individuals to access the information system from external information systems and process, store, or transmit USAID-controlled information using external information systems. This control recognizes that there are circumstances where members of the workforce using external information systems (i.e., contractors) need to access organizational information systems.
- Authorizing Officials (AO) must only authorize the use of external information systems to process, store, or transmit USAID-controlled information when USAID verifies the implementation of required security controls on the external system. For more information, see USAID Security Assessment and Authorization (SA&A) Process. This must be specified in the system security plan and in an approved information system connection agreement or similar agreements with the organizational entity hosting the external information system.

The Joint Financial Management System (JFMS) Service Level Agreement (SLA) Revision 1 states that:

- This SLA will be reviewed annually and modified as required to incorporate amendments that are necessary to support USAID and DoS requirements and to accurately reflect any changes. Any changes require the approval and signature of both USAID and DoS;

USAID has not updated its agreement with the DoS because they are awaiting an updated draft from the DoS. The agreement is a joint agreement that requires input and approval of both parties.

Weaknesses in the monitoring of third-party providers of information system services increase the risk that USAID management may not be aware of third-party security controls that are not adequately implemented or operating effectively which puts USAID at risk that its sensitive financial information may not be adequately protected. Additionally, AO and SO may not have adequate information to continuously monitor the status and effectiveness of information system controls to adequately address and accept risks on behalf of USAID.

<u>(B) Access Controls</u>

Access controls should provide reasonable assurance that computer resources (data files, application programs, and computer-related facilities and equipment) are protected against unauthorized modification, disclosure, loss, or impairment. During our audit, we noted two findings in this area.

2. Password controls should be strengthened

We noted the following weaknesses in the password controls for one system Application and its production and reporting databases:

- The password configurations for the reporting database supporting one system's application were not consistent with USAID policy. Additionally, one system Security Plan was not updated to document required deviations from USAID password policy. Specifically, we noted the following:

    - Password expiration was configured to 130 days for CONNECTFFS_PRO_Profile instead of 105 days (95 plus 10 grace time) required by the System Security Plan.
    - Password reuse max and reuse time is set to unlimited for the DEFAULT_PROFILE and CRITICAL_CONNECT_PROFILE profiles. This indicates that a user can reuse any password.
    - Account lockout threshold for the SERVICE_ACCOUNT Profile was set to unlimited instead of 3 failed attempts.

USAID's Automated Directive System (ADS) Chapter 545, Information Systems Security, states that, "*SOs must conform to the minimum requirements described below; however, SOs must determine whether higher level restrictions and conditions beyond these minimum requirements should be established in light of the risks involved with respect to the particular system. SOs must assure that the final restrictions and conditions are documented in the SSP.* "

"SOs must ensure the information system does the following regarding passphrases and password-based authentication:

1) *Enforces minimum password complexity of at least 12 characters, mix of at least one character from each of three of the following four-character types: upper-case letters, lower-case letters, numbers, and special characters;*
2) *Enforces at least the following number of changed characters when new passwords are created: four characters must be changed;*
3) *Stores and transmits only encrypted passwords;*
4) *Enforces password minimum and maximum lifetime restrictions, with no minimum lifetime and a maximum lifetime of 60 days;*
5) *Prohibits password reuse for 24 generations;*
6) *Allows the use of a temporary password for system logons only with an immediate change upon first-time logon to a new password; and*

The AC-2 control of one system's Financial System Security Plan (SSP) states:

"Password expiration is configured to 200 days for Critical Connect Profile and 70 days for the PHX_ADMPRO and DBAPRO Profiles instead of 190 and 60 days.

The USAID … ISSO has determined that 200 and 70 allows for better password management of the application-level accounts (CRITICAL_CONNECT profile). The risks to operations in changing application level passwords must be balanced against aging password risks. There is significant overhead in changing these passwords and the application itself must be offline during the process. The password change process must be scheduled on Saturdays. The 190 (Critical Connect) and 60 (PHX_ADMPRO, DBAPRO) day setting in addition to 10-day grace setting provides additional scheduling flexibility to allow us to keep to a fixed January/July schedule.

The new guidelines do not mention a required PASSWORD_GRACE_TIME in addition to the PASSWORD_LIFE_TIME. In the supporting database, PASSWORD_GRACE_TIME is set to 10 as was required.

Password expiration for all profiles within the reporting database except the service accounts profiles were changed from unlimited to 95 days. Additionally, password expiration for service accounts we configured to be changed once every 365 days. Service Account Profiles are set differently to allow for operational priorities to no impact application function as per the Oracle SOP and per USAID service account policies."

Based on discussions with USAID management, it was noted that corrective actions were initially taken; however, some of the password settings went out of sync because of a database patch update. Additionally, some of the profiles have settings that are necessary for the Extract Transfer and Load (ETL) process used to copy data from the production database to the data warehouse; however the System Security Plan was not updated to address these required deviations from USAID policy. Also, the patch management process did not include a verification to detect and resolve any instances where patch installations reset passwords settings.

Weakness in password controls increases the risk that unauthorized access to one system and its supporting databases may be compromised, thus putting systems and data at risk of unauthorized disclosure, modification, or destruction of data - possibly without detection.

3. Audit log reviews for one system and its supporting databases should be reviewed and analyzed in accordance with established policies

Audit log reviews of one system and its supporting databases are not being conducted in accordance with USAID's defined frequencies. Specifically,

- Audit logs for one system's application and its supporting production Oracle database show that they are reviewed monthly instead of daily as stated in the System Security Plan, or at least weekly as stated in ADS 545; and
- Audit logs for one system's reporting database are reviewed on an ad hoc basis when requested by application teams instead of daily, as mandated in the System Security Plan or at least weekly in accordance with ADS 545.

ADS Chapter 545, Information Systems Security section 545.3.4.6 Audit Review, Analysis, and Reporting (AU-6), states:

> "*SOs must ensure that audit records for Agency information systems are reviewed and analyzed at least weekly. This review and analysis must be documented as specified in the IA Audit and Accountability Guidance document. Unusual and suspicious activity or unexplained access attempts must be reported to the System or Mission ISSO, and a ticket opened with the M/CIO Service Desk at cio-helpdesk@usaid.gov."*
>
> *M/CIO must:*
>
> a. *Employ automated mechanisms to integrate audit review, analysis, and to support organizational processes for investigation and response to suspicious activities; and*
> b. *Provide a capability to analyze and correlate audit records across different repositories to gain organization-wide situational awareness*."

The AU-06 control of the Financial System Security Plan (SSP) states:

> "*Network and operating system level logs are controlled by Department of State and covered in the OpenNet SSP*.
>
> *Oracle and … logs of some types are reviewed daily. These are mostly account-related logs. Both Oracle and … transaction logs are reviewed on demand when necessary. Any items of note are passed on to … security or other appropriate parties for investigation.*
>
> *Logs review processes are reviewed as part of the annual security review process. Adjustments are also made when circumstances reveal a temporary need or a permanent change to risk or processes.*

> *Department policy requires ISSO staff to review and analyze information system audit records for systems under their control at least weekly"*

NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, requires that USAID:

a. Review and analyzes information system audit records [*Assignment: organization-defined frequency*] for indications of [*Assignment: organization-defined inappropriate or unusual activity*]; and
b. Reports findings to [*Assignment: organization-defined personnel or roles*].

We were informed that USAID reviews the system's application and production database log file daily and then monthly, provides continuous monitoring reporting to record that the reviews occurred. However, the continuous monitoring records do not demonstrate that the logs were reviewed daily. USAID will review the reporting template to see if it needs to be revised to better evidence that the reviews occurred daily instead of monthly.

Additionally, the system's reporting database logs were not reviewed because the CIOs office manages the database and CFOs Office performs the audit log reviews; however, USAID did not have a process to send the logs to the Information System Security Officer (ISSO) for review. The CFO's office is coordinating with the CIOs office to obtain an audit report from the reporting database that can be incorporated into the database review. This process is still ongoing.

Failure to review and analyzes information system audit records as required increases the risk that USAID may not be able to detect suspicious or unauthorized activity and respond to potential security events timely.