Anti-Fraud Field Guide: Implementing the USAID Anti-Fraud Plan

An Additional Help for ADS Chapter 596

New Edition Date: 12/13/2022
Responsible Office: M/CFO/ERM
File Name: 596sad_121322

INTRODUCTION

The Anti-Fraud Field Guide (Field Guide) supplements USAID's Anti-Fraud Plan issued in February 2021 in accordance with the Government Accountability Office (GAO) Framework for Managing Fraud Risks in Federal Programs (GAO Fraud Risk Framework). The Anti-Fraud Plan supports Assessable Units (AUs) to ensure they identify and address fraud risks as an integral part of the Agency's Enterprise Risk Management (ERM) program.

This Field Guide provides guidance to operationalize and implement the Agency's Anti-Fraud Plan and highlights how existing tools and processes at USAID can be tailored to implement anti-fraud activities at the AU and program specific level (see Mission Enterprise Risk Management Systems that include Quarterly Financial Reviews, Portfolio reviews, and Monitoring and Evaluation already in place). The Field Guide follows a risk-based approach to assess, design, and implement control activities that mitigate fraud risks. Specifically, this guidance provides recommendations to AUs, including USAID Missions, in applying fraud risk guidance and the tools available for conducting Fraud Risk Assessments. AUs are best placed and most knowledgeable about the Mission, country context, and pertinent program priorities to adopt the Field Guide and own the process to implement the Anti-Fraud Plan. For this reason, and based on the GAO Fraud Risk Framework recommendations, successfully implementing the Field Guide should not be prescriptive, but flexible and tailorable.

BACKGROUND

The Office of Management and Budget (OMB) **Circular A-123 Management's Responsibility for Enterprise Risk Management and Internal Control** defines *risk* as the "effect of uncertainty on [an Agency's] objectives."

USAID defines risk within the context of the Agency **Risk-Appetite Statement (RAS)**. The RAS addresses a full spectrum of risks and manages their combined impact as an interrelated risk portfolio. The RAS provides a higher-level statement on the levels of risk USAID deems allowable for the key risk categories, and helps technical teams set the acceptable level of variation around project objectives within each category. As an integral part of the Agency's ERM program, the Anti-Fraud Plan aligns with the components of the GAO Fraud Risk Framework for effectively identifying and managing fraud risks, as well as enhancing protocols to increase fraud awareness and address confirmed incidents of fraud.

The components of the GAO Fraud Risk Framework include:

Figure 2: The Fraud Risk Management Framework

Source: GAO. | GAO-15-593SP

Component 1

Component 2

Component 4

Component 3

Component 1. Commit: Pledge to combat fraud by creating an organizational culture and structure conducive to managing and reducing the risk of fraud.

Component 2. Assess: Plan regular fraud risk assessments and assess them to determine a risk profile.

Component 3. Design and Implement: Design and implement a strategy with specific control activities to mitigate assessed fraud risks and collaborate to help ensure their effective implementation.

Component 4. Evaluate and Adapt: Evaluate outcomes by using a risk-based approach and adapt activities to improve the management and reduction of fraud.

ROLES AND RESPONSIBILITIES

The Anti-Fraud Plan acknowledges the responsibilities/functions of USAID's personnel and integrates anti-fraud processes with existing internal controls and risk-management processes

and tools. AUs can also use the illustrative roles and responsibilities matrix to delineate the roles and responsibilities within an AU in preventing, detecting, and responding to both external and internal parties.

Some best practices on roles and responsibilities include:

- Demonstrate senior level commitment to combat fraud that is inclusive of all staff. Mission Directors should consider designating an office to lead fraud risk management activities.

- Ensure Mission staff have defined responsibilities and necessary authority to serve its role. Please see the following notices, as examples: Executive Notice - USAID Commitment to Report Fraud in our Country Programs; USAID Launches Anti-Fraud Plan; Funds Control Requirements.

- Top-down messaging from senior management and officials should be done at least bi-annually.

- Reference the GAO Greenbook, which indicates fraud prevention and internal control is the responsibility of everyone in the entity.

The following include roles and responsibilities sections for GAO and OMB:

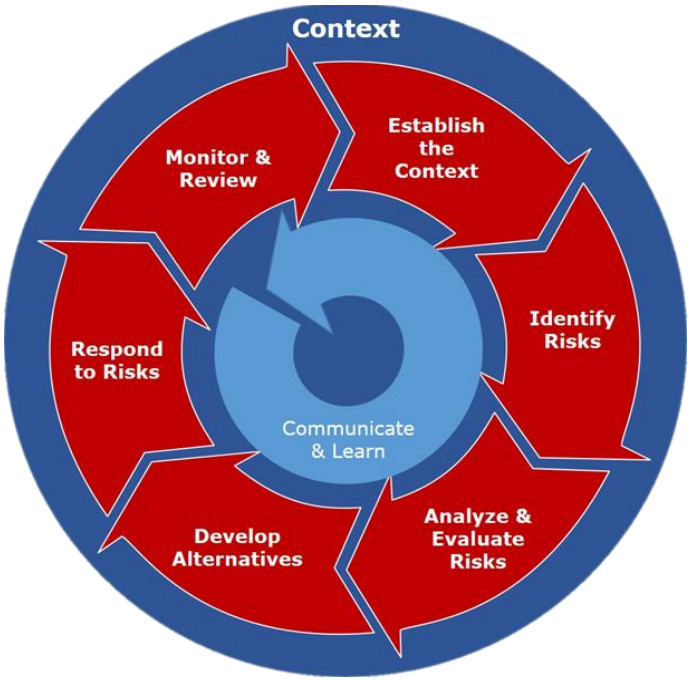
- Government Accountability Office's (GAO) Standards for Internal Control in the Federal Government, and

- Office of Management and Budget (OMB) Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control.

HOW USAID'S ENTERPRISE RISK MANAGEMENT PROCESS ALIGNS WITH THE GAO FRAUD RISK FRAMEWORK

The USAID ERM (Risk Management) Process

The Agency has adopted the seven-step risk management process defined in and adapted from OMB Circular A-123. The risk management process is not meant to be a stand-alone activity, rather, it is a framework or approach to use in decision-making processes. The steps below must be performed in sequential order to properly address and manage risk for an organization:



The following table shows the alignment of USAID's ERM Process with the GAO Fraud Risk Framework.

USAID's ERM Process (Risk Management)	GAO Fraud Risk Framework
Step 1 – Establish the Context In this step Missions: ● Learn about the given environment and how systems work. ● Learn about fraud risk factors or conditions/uncertainties in the systems that could pose risks. ● Consider policy concerns, operating units' organizational needs, and establishing the Mission's defined responsibilities and authority to serve its role. Therefore, setting the context is key to be able to continue with fraud risk assessment steps.	**Component 1 – Commit**
USAID's ERM Process (Risk Management)	**GAO Fraud Risk Framework**
Step 2 – Identify Risks **Step 3 – Analyze and Evaluate Risks** **Step 4 – Develop Alternatives** Missions should continue with their regular fraud risk assessments (see the	**Component 2 - Assess**

Example_Fraud_Risk_Assessment (1).xlsx). The creation of a risk profile offers a method for systematic identification and documentation of risks.

USAID's ERM Process (Risk Management)	GAO Fraud Risk Framework
Step 5 – Respond to Risk	**Component 3 – Design and Implement**

In this step, Missions implement specific control activities to mitigate the fraud risk. Actions used to fight fraud include but are not limited to: vigilance, setting the tone, fraud awareness training, accountability, assessing risks, establishing written procedures, reviewing internal controls, adequate segregation of duties, and monitoring for clues.

Report any fraudulent activities or suspected fraud to the USAID Office of the Inspector General (OIG) Hotline Number: +1-202-712-1023; +1-800-230-6539; Hotline WhatsApp: +1-202-704-2160; or email: ig.hotline@usaid.gov.

USAID's ERM Process (Risk Management)	GAO Fraud Risk Framework
Step 6 – Monitor and Review	**Component 4 – Evaluate and Adapt**

In this step, Missions evaluate the actions taken to mitigate fraud risks and adapt or modify them if needed. This step is a continuous process.

USAID's ERM Process (Risk Management)	GAO Fraud Risk Framework
Step 7 – Communicate, Learn, and Adapt	**Component 1 – Commit** **Component 4 – Evaluate and Adapt**

In the final step, once Missions have implemented, monitored, and reviewed activities to improve fraud risk management, they should collect and analyze data to review trends and use the results of monitoring to provide oversight for fraud prevention, detection, response, and update training to align with new procedures. As provided in the Agency Anti-Fraud Plan, training will be provided both internally and to Agency implementing partners.

An Example of Applying the Risk Management Framework

The Agency's risk management on fraud detection in Global Health Supply Chain contracts is a valuable example of the application of the risk management process. The Agency's Risk Management Council (RMC) and the Executive Management Council on Risk and Internal Control (EMCRIC) managed risks related to project performance, which incorporated a need to monitor the potential risk of fraud or loss in USAID supply chains.

In response, USAID developed a fraud risk model to identify, prioritize, mitigate, and monitor supply chain risks. In addition, 31 USAID staff from 26 countries reviewed tools and best practices, and developed guidelines to create a proactive collaborative approach, which included a Supply Chain Activity Manager(s) and Mission Risk Management Liaisons (RMLs). This integrated approach ensures that the agency can identify and mitigate supply chain vulnerabilities and potential risks including fraud, abuse and/or missue, counterfiet activities, and the diversion of products and financial resources.

MANAGING FRAUD RISKS USING ENTERPRISE RISK MANAGEMENT PROCESSES

The Agency's seven step risk management process is intended to be used as a Mission plans, assesses, responds to, and monitors and evaluates fraud risks. The Agency's RAS details risk-tolerance levels and categories of risk in support of U.S. foreign policy, national security, and humanitarian and disaster assistance objectives. The risk management process encourages taking smart risks in an informed and documented manner that balances risk levels with potential opportunities. The seven steps are explained below along with tools available (***not all inclusive***) to implement the process:

Process	Tools

Step 1 - **Establish the Context.** The first step is to set goals and objectives, then determine the requirements, constraints, and opportunities that will influence the process. Context setting also includes assigning responsibilities within the risk management process, defining the scope of risk management activities, and defining risk assessment methodologies. The context includes the significant factors that affect the ability of a Mission or Washington Operating Unit (OU) to achieve its goals or strategic objectives. It may also include goals and objectives occurring on the operational level. Finally, establishing the context involves considering policy concerns and OU and organizational needs.	• Anti-Fraud Plan and Message
	• Current and Relevant reports
	  ○ Mission Risk Profiles
	  ○ Internal/External Assessments and Mandatory Analyses (e.g., OMB A-123 Assessment)
	  ○ Audit Reports
	  ○ Donor Assessments
	  ○ Country Development Cooperation Strategy (CDCS)/Regional Development Cooperation Strategy (RDCS)
	• Federal Managers' Integrity Act (FMFIA) certifications
	• Government Management Reform Act (GMRA) audits

Step 2 - **Identify Risks**. Risk identification is a structured process to recognize the potential for undesired	• Uniform Risk and Internal Control Assessment (URICA) Tool for OMB A-123 reporting

Process	Tools
outcomes or possible opportunities. Managers and subject matter experts, who are closest to programs and functions and are most knowledgeable about the risks faced, should serve as the primary source for identifying fraud risks. The identification of risks can generally be done from a basic knowledge of the subject matter and understanding of the desired outcome. The context, defined in the previous step, should help inform which risks are identified. An identification and review of risks should also evaluate the potential opportunity for improving the effectiveness of existing processes and programming. From an internal control perspective, the annual FMFIA assessments and the OMB A-123 assessments are potential avenues to identify risks.	• Mission Enterprise Risk Management Systems • USAID OIG Fraud Questionnaire • GAO Standards for Internal Control • OMB A-123 (Appendix A, B, C, and D) Reviews • FMFIA certifications • Federal Information Security Modernization (FISMA) Act audits • Non-U.S. Pre-award Surveys (NUPAS) • CDCS • Government-to-Government Risk Assessments • Capacity Assessments • Audits (e.g., GMRA, Defense Contract Audit Agency (DCAA), Cost Accounting Standards (CAS) Disclosure Statement Audits, Systems, Single Audit Act, and Audit Close Out) • GMRA • Other Reviews (e.g., financial, non-financial, payment integrity, suspension and debarment program) • Pre-award Surveys per 2 CFR 200 • Agency Monitoring and Evaluation Reviews Available Information (e.g., document reviews, data matching after payments have been made, site visits, and data mining and use of data analytics tools)
Step 3 - **Analyze and Evaluate Risks.** Risks identified in the previous step undergo analysis and evaluation. Risks are rated/scored based on the probability or likelihood of the risk materializing plus the impact/consequence that risk could have on activity performance. An analysis of risks can help prioritize and focus planning, monitoring, and reviews.	• Example_Fraud_Risk_Assessment (1).xlsx
Step 4 - **Develop Alternatives**.	• Agency Risk-Appetite Statement

Process	Tools
Missions develop risk mitigation strategies/measures to address all identified risks. The goal of this step is to provide decision makers with a structured approach to identify and choose risk mitigation actions. As stated in the RAS, for fiduciary risks, which are events or circumstances that could result in fraud; waste; loss; or the unauthorized use of U.S. Government funds, property, or other assets, the risk appetite is low. Because fiduciary risk appetite is low, the Agency implements rigorous safeguards against fraud, corruption, or diversion of funds; continually maintains, assesses, and updates its systems of audit, risk assessment, and internal controls; and identifies additional mitigation measures as needed in agreements with the partner country, such as complementary anti-corruption programming or enhanced controls.	● Example_Fraud_Risk_Assessment (1).xlsx
Step 5 – **Respond to Risks**. The response/action identified in step four is selected as the most appropriate option to put into effect. This is the "decide and implement" phase where decision makers should consider the strengths and weaknesses of the various alternatives and consider practical restraints such as time, resources, and capacity. Decision makers will also want to consider legal issues, the potential impact on stakeholders, and any additional or new risks that may be created in the response process.	The responses are outlined in the GAO Standards for Internal Control Principle 7.08, for example: ● **Accept** means no action is taken to respond to the risk based on the insignificance of the risk. ● **Reduce** refers to an action that is taken to reduce the likelihood or magnitude of the risk. ● **Share** suggests an action is taken to transfer or share risks across the entity or with external parties to ensure against loss. ● **Avoid** indicates an action is taken to stop some or all the operational process causing the risk. Risk mitigation strategies include:

Process	Tools
	• Segregation of Duties • Employee Background Checks • Payment Recovery • System Edit Checks, Data Matching • Recommendations and Responses (e.g., financial and non-financial audits/reviews/surveys) • FISMA/Cybersecurity assessments
Step 6 - **Monitor and Review.** There should be regular monitoring, reviewing, and updating (if necessary) of the documented risk information, from the context, identification, analysis, alternatives, and responses. The review should seek to determine whether risk responses are addressing risks as intended and identify when changes are needed. When implementing a risk response, context (including the internal USAID environment and the external context) and performance (included within the logic model) should be monitored periodically. If there is a change in context, the response may need to be altered. If the response is not having the desired effect, it may need to be adjusted.	Monitoring is a key component for fraud risks and monitoring audit findings, evaluations, audits, and investigations will assist in achieving stated goals. Tools include: • Comparisons • Reconciliations • Automated Tools • Investigating Complaints • Establishing Clear Reporting Hierarchy
Step 7 - **Communicate, Learn, and Adapt.** Risk management is an iterative process, occurring continually throughout the year. It is important to periodically reflect on the risk management process in action and determine if there should be changes in the approach or practice. Best practices and lessons learned in the risk management process should be shared and communicated across the Agency, and when appropriate, with stakeholders. Information communicated will vary between audiences, especially	• Communicate a "tone from the top" message on fraud prevention (see the Commitment with the ERM/IC Governance Culture: Tone from the Top Executive Message) regularly. • Develop a plan (using the Agency Anti-Fraud Plan) based on the country context, program parameters and/or local conditions and widely communicate. • Applying lessons learned and best practices from Steps 1-6. • Developing USAID-Mission specific training. For example,

Process	Tools
between internal and external groups. This step also includes training that communicates the importance of fraud awareness and the anti-fraud strategy in Mission Directors' and Office Directors' regular communications to staff.	● USAID OIG can provide training upon request and availability. ● USAID/Egypt Financial Management Services Unit (FMSU) Course - Can be requested using the Compliance and Capacity Development Training (CCD) - Request Form & Financial Management Services Request Form ● Management Concepts, Overview of GAO Requirements for Fraud Prevention, ERM, and Internal Control https://www.managementconcepts.com/course/id/5892 ● On-site Delivery of Association of Certified Fraud Examiners (CFE) management training on Fraud Risk ● Association of Government Accountants (AGA) Fraud Risk Training and Tools ● Issuing continuous messages on the importance of preventing and managing the risk of fraud (e.g., Mission notices, messages, videos, webinars/presentations with local partners). ● Collecting and analyzing data on detected fraud schemes to improve fraud prevention controls.

INTERNAL & EXTERNAL REFERENCES AND SOURCES OF INFORMATION

ERM Risk Profile Implementation Guide: Missions may use their Annual Risk Profile to see identified and documented key risks and weaknesses in internal controls.

FMFIA certification Website: The FMFIA certification may be used to see USAID identified and documented key risks and weaknesses in internal controls.

Agency Financial Reports: The report's findings are a key driver for continuous fraud-related and risk management monitoring activities. Missions may refer to the top management challenges included in the AFRs.

Annual USAID Government Management Reform Act of 1994 (GMRA): Fraud is an area of consideration during the GMRA audits. GMRA considerations of fraud covers the following: (1) procedures, if any, which management has established to identify, account for, and disclose related party relationships and transactions; and (2) controls in place to prevent/detect fraud in projects managed by the Mission, and controls over approving travel, issuing advances, and review of travel vouchers. In addition, the GMRA audit includes common findings related to: accruals, advances, disbursements, improper payments, budget and obligations, fund balance with treasury and e-cart reconciliation, accounts receivable, data calls, credit programs, cashier (imprest funds) operations, and local currency trust funds management.

Internal Fraud References

USAID OIG Compliance and Fraud Prevention Guide for Program Implementers

USAID Anti-Fraud Risk-Management Message

USAID Governance Charter for Enterprise Risk Management and Internal Control: ADS 596mab

USAID Mission Risk Management Systems

ERM and Internal Control Governance Structure

Fraud Prevention and Compliance Handbook

OIG Office of Inspections and COVID-19 Fraud Reporting

Copy of COVID Fraud Awareness - COVID-19.pdf

USAID's Acquisition Regulations (AIDAR)

External Fraud References

2 CFR 200, Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards

Federal Acquisition Regulations (FAR)

Federal Managers' Financial Integrity Act (FMFIA) of 1982

Federal Financial Management Improvement Act (FFMIA) of 1996

Federal Information Security Modernization Act (FISMA) of 2014

Federal Information Technology Acquisition Report Act (FITARA)

Government Performance Results Act (GPRA) Modernization Act of 2010

The Fraud Reduction and Data Analytics Act of 2015

Office of Management and Budget (OMB) Circular No. A-123, Management's Responsibility for Enterprise Risk and Internal Control (2016) and its Appendices

Payment Integrity Information Act of 2019

US Department of the Treasury, *Do Not Pay Initiative*

Program Integrity -Treasury Anti-Fraud Playbook

GAO Framework for Managing Risk in Federal Programs

GAO Standards for Internal Control in the Federal Government (GAO Green Book)

GAO Data Analytics to address Fraud and Improper Payments

Association of Certified Fraud Examiners (ACFE) Resources

Fraud-Risk Fundamentals

Fraud-Risk Decision Tree

Sample Fraud-Risk Assessment

APPENDIX 1 – Examples of the USAID's Risk Management Process

Example 1 – The G2G Risk Management Process

The G2G Risk Management process aligns with the Agency's seven step risk management process. G2G Risk Management examines the current processes, capacity, control systems, and day-to-day practices used in a specific partner country, ministry, district, or agency that would be responsible for managing USAID funding with a particular activity. This examination needs to include: (1) appropriate testing of the systems to validate operations; (2) identification of vulnerabilities; (3) developing alternatives that influence the appropriate risk treatment measures; and (4) responding to risks while developing a risk mitigation plan that is finalized during activity design. Armed with this analysis, the Mission is best positioned to respond to the most significant or severe threats or maximize opportunities.

Example 2 – Risk Response

Annual risk-based assessments are performed under the 2008 Negroponte Directive. These assessments ask Missions to consider steps that should be taken to ensure that USAID funding and assistance is not diverted to terrorist groups.

Development Innovation Ventures (DIV) in the U.S. Global Development Lab responded to risks associated with a grant that tested the cost effectiveness of unmanned aerial vehicles for delivery of health products. DIV awarded a grant to Vayu, to deliver health products, originally in rural Kenya. Since the technology was relatively new and unregulated, DIV managed a risk by requiring regulatory approval from all relevant Kenyan ministries as the first milestone towards payment. Vayu did not receive full approval by Kenyan authorities, so the treatment of the risk was not successful. To compensate and continue to treat the identified risk, the project was shifted to Madagascar, where officials gave permission to test its technology. The shift in location was key and allowed the project to respond to the increased risk of not receiving full approval in Kenya, while implementing their treatment option of receiving host government approval.

Example 3 – Monitoring and Review

USAID/Washington manages a monitoring and review process for the Agency's programs occurring in countries designated as Closed Spaces. The process includes quarterly reviews where all non-humanitarian assistance programs are assessed to make sure they are continuing to strike the proper balance between security and transparency amidst political shifts and other potential risks. All new activities are reviewed immediately to ensure they are following the USAID Guidance on Programming in Closed Spaces. Twice a year, the Deputy Administrator convenes a meeting for Agency leaders to share and discuss issues raised in quarterly and hoc reviews of Closed Space programming and to consider whether there are any additional countries that qualify as a Closed Space.

APPENDIX 2- Examples of Fraud Risk Identification

The examples included in Appendix 2 are from the FY2020 Agency Financial Report under the Office of Inspector General's Statement of Most Serious Management and Performance Challenges for USAID.

Example 1 - Insufficient award management also creates opportunities for fraud

OIG investigation exposed fraud and conflicts of interest affecting a $4.7 million USAID-funded agriculture program in Uganda. OIG's investigation uncovered a conflict of interest involving consultancy contracts awarded to the implementer's former chief of party as well as evidence that the project accountant falsified records to substantiate payments. In January 2020, the implementer responded by instituting various organization-wide process improvements, including anti-bribery policies, and revising and updating policies for reporting ethical misconduct, whistleblower protection, conflicts of interest, and document retention. Two other multiyear investigations revealed extensive fraud and abuse by an implementer of multiple USAID grants and contracts. The implementer's senior leadership intentionally charged unallowable costs to its indirect accounts, including the funding of lavish off-site retreats, unallowable public relations costs incurred solely to promote the organization, and large year-end bonuses for senior managers at the organization. We questioned $17.3 million in direct and indirect costs incurred by the implementer between 2009 and 2014; in February 2020, USAID issued a bill of collection to the implementer for $5.5 million of the incurred costs.

Example 2 - Pandemic - Exacerbated Challenges

Detecting and Preventing Fraud in complex environments. The flow of substantial funding into crisis environments creates prime opportunities for fraud. Audits and investigations have exposed instances where individuals and organizations take advantage of American generosity through diversions of USAID-funded goods, contract steering, bid rigging, and other acts of corruption. Our monitoring of overseas contingency operations indicates that bad actors could exploit oversight gaps created by the pandemic to recruit fighters, prepare attacks, restrict civilian access to information about the pandemic, or divert life saving commodities.

For example, according to the Combined Joint Task Force – Operation Inherent Resolve, temporary increases in the Islamic State of Iraq and Syria's pace of attacks in Iraq likely indicated an "opportunistic exploitation of a confluence of factors," such as the Iraqi Security Forces' "preoccupation" with measures to contain COVID-19. The World Health Organization (WHO) similarly reported that the rise of COVID-19 cases in Africa presents an unprecedented challenge to U.S. counterterrorism and counter-violent extremism efforts.

While USAID prohibits implementers from engaging with sanctioned entities and requires prompt reporting of fraud and other allegations of wrongdoing, USAID faces challenges in detecting and preventing misconduct, as our recent responsibility referrals have highlighted. In one case, a U.S.-based implementer knowingly failed to disclose credible allegations of procurement fraud committed by sub-awardees in its programs. In another case, a non-

governmental organization based outside of the United States refused to provide requested records to OIG and other U.S. Government officials within a reasonable timeframe during an investigation into whether the organization had concealed past material support to designated terrorist organizations when applying for USAID awards.

The Agency must hold implementers accountable for non-cooperation with OIG investigations or risk setting a troubling precedent for the Agency's ability to obtain and respond to facts suggesting fraud and corruption in USAID programming. We have an ongoing audit looking at fraud risk management in the Agency's humanitarian programming for the Venezuela crisis and the challenges USAID faces in its response. We are also auditing USAID's oversight of an implementer in Syria and the effectiveness of corrective action taken for fraud risks we identified in cross-border activities.

APPENDIX 3 - Risk Response Examples

The examples included in Appendix 3 are from the FY2020 Agency Financial Report under the Office of Inspector General's Statement of Most Serious Management and Performance Challenges for USAID.

Example 1 - Risks for Unreported Fraud and Aid Diversions Involving Public International Organizations in Humanitarian Settings

In September 2018, USAID's Agency Financial Report reported that USAID's policy for public international organizations (PIOs), organizations principally made up of multiple governments or international financial institutions, did not align with Federal internal control standards. USAID frequently relies on PIOs such as the World Food Programme (WFP) to implement its humanitarian programs in nonpermissive environments. In response to recommendations, USAID adopted measures to improve PIO oversight, including a standard award provision for PIO awards, in November 2019, with a requirement to report fraud and misconduct allegations directly to OIG. While progress has been made, implementation of protocols to effectuate, communicate, and streamline the new requirement is still needed to ensure PIOs report allegations to OIG as required. By the end of September 2020, OIG had received five direct disclosures of alleged fraud and misconduct from PIOs, per the new requirements—a start in improved direct reporting but a figure judged to be low given the size and scope of USAID's PIO awards. Using WFP diversions in Yemen as a case study, we have ongoing work that reveals lessons learned and continuing challenges for USAID in working through PIOs, including obstacles to responding to limitations in access, information sharing, and transparency in humanitarian settings, as well as the need for increased coordination between humanitarian assistance donors and PIOs. USAID has taken steps to overcome or mitigate obstacles in these areas, including establishing a Response Management Team in February 2020 to coordinate the U.S. Government response to continued impediments to humanitarian access in Yemen, but opportunities remain to further reduce the risk of diversion and ensure aid reaches those who most need it.

Example 2 - Actions to Manage Risks Inherent to Humanitarian and Stabilization Assistance

COVID-19 examples of these activities include assessing implementers' proposed plans for providing humanitarian assistance in the pandemic context, including plans for procuring and distributing commodities, and coordinating with other USAID Bureaus and other agencies such as the State Department. For high-threat operating environments, USAID requires implementers to submit risk mitigation plans, which specifically examine internal control systems. In addition, USAID noted a requirement for all potential implementers to include in their applications fraud prevention measures, as well as the guidelines they plan to implement for managing COVID-19 risks. Coordinating with OIG to provide training to implementers is another piece of USAID's strategy to ensure implementers promptly report and follow up on all instances of fraud and other programmatic irregularities.

Example 3 - Actions to Prevent Fraud, Waste, and Abuse

Recent and ongoing investigations highlight how gaps in planning, monitoring, and risk mitigation can result in performance shortfalls that go unchecked and create opportunities for bad actors to pilfer USAID funds and commodities for personal gain. Please see the following examples:

- USAID's $9.5 billion Global Health Supply Chain – Procurement and Supply Management (GHSC-PSM) Project—the largest component of USAID's $10.5 billion GHSC program—has been under scrutiny since 2016, when investigations revealed that partner governments were either unable or unwilling to put in place controls that would minimize the potential for large-scale, illicit resale of USAID-funded commodities to private businesses and public markets. In two ongoing investigations against one USAID implementer, OIG confirmed the theft as well as transnational and transcontinental diversion of USAID-funded health commodities from USAID programs in Kenya, Tanzania, Uganda, and other countries in Africa to countries in South America, the Caribbean, and potentially elsewhere. The OIG investigations determined that system weaknesses, a lack of implementer internal controls, and potential corruption at the highest levels of the implementing organizations created supply chain vulnerabilities. In coordination with USAID and law enforcement partners, we are pursuing additional GHSC-PSM casework in Kenya.
- USAID's $72 million education program in Rwanda was subject to procurement fraud when a subcontractor's managing director sought to bribe a USAID employee for procuring sensitive information. USAID debarred the managing director and received specific commitments from the subcontractor to implement an anti-bribery and anti-corruption policy.
- An OIG investigation determined that a USAID implementer in Egypt inflated the number of beneficiaries receiving training and technical assistance under a USAID-funded agricultural program. However, OIG's investigation also found that USAID wrote the award in a manner where payments to the implementer were not contingent on the number of beneficiaries reached. In November 2019, the USAID mission in Egypt made staff changes and implemented new procedures, such as strengthening monitoring and evaluation systems and project oversight, to identify and prevent future schemes.
- OIG investigations have also exposed multiple cases of billing fraud against USAID awards. In one case, an implementer working under a project that sought to increase health programs in the Philippines mischarged USAID over $42,000 for employee work and lodging expenses unrelated to the USAID project, which USAID issued a bill of collection for, in February 2020. In another case, an implementer's engineering consultant and contractors submitted falsified documents to obtain USAID funding under a construction project in Uganda.

Example 4 - Prudently Managing Pandemic-Related Acquisition and Assistance (A&A) Procurement and Reporting Flexibilities Instituted to Provide Rapid Response

New A&A flexibilities for the pandemic response temporarily waive requirements for competition, source, and nationality of goods and services, and temporarily expand A&A and

purchasing capabilities of non-U.S. direct-hire personnel. Federal guidance provides additional temporary relief for administrative, financial management, and audit requirements. These measures, which enable USAID to act swiftly and offset risks its implementers may face during a public health emergency of international concern, require a different approach to fiscal prudence. For example, USAID acknowledges the need to implement controls to ensure that OUs do not use A&A flexibilities to extend poorly performing programs; sign agreements with unqualified recipients; or circumvent competition, source, and nationality requirements for ineligible programs, goods, and services. The Agency also recognizes the need to provide training and supervisory oversight for staff taking on new A&A-related responsibilities. USAID reported working to publish clear and effective guidance on programming and funding processes for staff and implementers and has released supplemental information where existing guidance is incomplete. However, the shifted and constrained management structure of staff working from alternate locations under new expectations and evolving guidance will continue to challenge USAID oversight and may increase risks of introducing inefficiencies by well-meaning staff and fraud by bad actors who seek to exploit the crisis for personal gain.

For example, prior to the pandemic, our investigation confirmed that multiple Foreign Service National employees at USAID's Southern Africa mission were involved in a contract-steering conspiracy. One employee registered a shell company that received ten USAID contracts over the course of four years valued at more than $150,000. Two additional employees knowingly fabricated quotes, invoices, and reports in support of the scheme. The three confessed to taking kickbacks on contracts awarded to the shell company and admitted that USAID received little to no goods under these contracts. In November 2019, following an OIG referral, USAID terminated employment for the three conspirators for fraud and theft, while a fourth individual implicated in the investigation resigned in lieu of termination.

Other instances of A&A fraud have resulted in numerous USAID and implementer staff terminations and resignations. One investigation in Liberia found that implementer employees steered over $1.5 million of the $9.5 billion GHSC-PSM award to a vendor with falsified documentation. In Nepal, a Foreign Service National and an employee of a USAID GHSC-PSM contractor were implicated in improperly disclosing A&A sensitive information for a USAID-funded subaward to a prospective bidder. In Zambia, OIG substantiated allegations that the lead engineer of an implementer under the GHSC-PSM award violated the implementer's conflict of interest policy and shared A&A-sensitive information with a prospective vendor.

APPENDIX 4 - Key Definitions

Assessable Unit (AU): An organizational unit within USAID, i.e., Mission, Bureau, or Independent Office, that is required to submit an annual Statement of Assurance on the status of internal control and a Risk Profile to the next management level. All Missions, Bureaus, and independent offices are AUs. Additionally, lower-level organizational units can be AUs, as designated by the responsible Bureaus/Independent Offices/Missions. **(Chapter 596)**

Bribery: The offering, giving, receiving, or soliciting of anything of value to influence an official act or business decision (see Association of Certified Fraud Examiners [ACFE]).

Coercive practices: Impairing or harming, or threatening to impair or harm, directly or indirectly, any party or the property of the party to influence improperly the actions of a party.

Collusive practices: An arrangement between two or more parties designed to achieve an improper purpose, including influencing improperly the actions of another party.

Conflict of Interest: An undisclosed personal or economic interest that an employee or agent has in a transaction that adversely affects his or her professional role (see ACFE).

Corrupt practice: The offering, giving, receiving, or soliciting, directly or indirectly, of anything of value to influence improperly the actions of a public official.

Corruption: The wrongful use of influence to procure a benefit for the actor or another person, contrary to their duty or the rights of others (see ACFE).

Economic Extortion: When an employee or official, through the wrongful use of actual or threatened force or fear, demands money or other consideration to make a business decision (see ACFE).

Fraud: Obtaining something of value through willful misrepresentation Whether an act is in fact fraud is a determination to be made through the judicial or other adjudicative system and is beyond management's professional responsibility for assessing risk. (Chapter 596, Government Accountability Office Standards for Internal Control in the Federal Government ["Green Book"]. Source: ADS 308mab M.17 Fraud, Corruption, and Other Prohibited Conduct (November 2019)

Fraudulent practice: Any act or omission, including misrepresentation, that knowingly or recklessly misleads, or attempts to mislead, a party to obtain a financial or other benefit, or to avoid an obligation.

Obstructive practices: Deliberately destroying, falsifying, altering or concealing of evidence material to the investigation or making false statements to investigators in order to materially impede a recipient investigation into allegations of a corrupt, fraudulent, coercive, or collusive practice; threatening, harassing or intimidating any party to prevent it from disclosing its

knowledge of matters relevant to the investigation or from pursuing the investigation; or acts intended to materially impede the exercise of recipient's contractual rights of audit or access to information.

APPENDIX 5 - Forms of Fraud

GAO Standards for Internal Control in the Federal Government ("Green Book"):

Corruption: Bribery, conflicts of interest, illegal gratuities, and other illegal acts, i.e., economic extortion.

Fraudulent Financial Reporting: Intentional misstatements or omissions of amounts or disclosures in financial statements to deceive the users of the financial statements. This could include the intentional alteration of accounting records, the misrepresentation of transactions, or the intentional misapplication of accounting principles.

Misappropriation of Assets: Theft of an entity's assets, which could include the theft of property, the embezzlement of receipts, or fraudulent payments.

596sad_121322