OFFICE OF INSPECTOR GENERAL

AUDIT OF AUDIT OF USAID/ WEST BANK AND GAZA'S PARTNER VETTING AND GEO-MANAGEMENT INFORMATION SYSTEMS

AUDIT REPORT NO. 6-294-14-007-P
APRIL 23, 2014 [Revised]

CAIRO, EGYPT

Office of Inspector General

April 23, 2014

MEMORANDUM

TO: USAID/West Bank and Gaza, Mission Director, R. David Harden
USAID/Office of Security, Division Chief, David Blackshaw

FROM: Regional Inspector General/Cairo, Catherine Trujillo /s/

SUBJECT: Audit of USAID/West Bank and Gaza's Partner Vetting and Geo-Management Information Systems (Report No. 6-294-14-007-P)[REVISED]

This memorandum transmits our final report on the subject audit. We have considered your comments on the draft report and included them, without attachments, in Appendix II.

The final report contains 37 recommendations to help USAID/West Bank and Gaza improve its implementation and use of the Partner Vetting and Geo-Management Information Systems. In its comments on the draft report, USAID/West Bank and Gaza agreed with 36 recommendations and disagreed with 1. Based on our evaluation of management comments, we acknowledge that the mission made a management decision on all 37 recommendations and has taken final action on Recommendations 14, 21, 23, 25, 28, 33, and 35. Please coordinate final action for the remaining recommendations with the Office of Audit Performance and Compliance Division.

Thank you for the cooperation and assistance extended to the audit team during this audit

U.S. Agency for International Development
USAID Office Building
1/A Nady El-Etisalat St.,
off El-Laselki St
New Maadi
Cairo, Egypt
http://oig.usaid.gov

CONTENTS

Abbreviations

The following abbreviations appear in this report:

ADS	Automated Directives System
AOR/COR	agreement officer's or contracting officer's representative
COBIT	Control Objectives for Information and Related Technology
FIPS	federal information processing standards
FISMA	Federal Information Security Management Act of 2002
Geo-MIS	Geo-Management Information System
HTTPS	hyper text transport protocol secure
IT	information technology
NGO	nongovernmental organization
NIST	National Institute for Standards and Technology
PIF	partner information form
PVS	partner vetting system
SSL	secure socket layer
RIG	Regional Inspector General
SP	Special Publication

SUMMARY OF RESULTS

The Federal Information Security Management Act of 2002 (FISMA) requires agencies to implement an agency-wide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or source. The act also requires an annual assessment of their information systems.

In response to FISMA requirements, National Institute for Standards and Technology (NIST) developed mandatory federal information processing standards (FIPS) 199, "Standards for Security Categorization of Federal Information and Information Systems," and 200, "Minimum Security Requirements for Federal Information and Information Systems" to help all federal agencies comply with FISMA. As part of its Special Publication (SP) 800-53, NIST established guidelines for selecting and specifying security controls for organizations and information systems to help federal government executive agencies meet the requirements of FIPS 200.

USAID/West Bank and Gaza uses three information systems described below to support implementation and monitoring of its programs.

Partner Vetting System

Following the events of September 11, 2001, President George W. Bush issued Executive Order 13224, "Blocking Property and Prohibiting Transactions with Persons Who Commit, Threaten to Commit, or Support Terrorism," effective as of September 24, 2001. This order identifies certain people and entities that the United States is prohibited from dealing and entering into transactions with. In addition, this order authorizes the Secretaries of State and Treasury to designate additional individuals and entities subject to the order.

The purpose of this policy was to make sure the U.S. Government did not inadvertently provide funding to a terrorist organization. Under the policy, people and organizations that USAID was considering issuing awards to had to go through a screening process called vetting—in which a person or entity is investigated for links to terrorism.

In August 2003 USAID/West Bank and Gaza issued its first comprehensive policy to address the requirements of Executive Order 13224. In March 2006 it updated that policy by issuing Mission Order No. 21, establishing criteria requiring non-U.S. organizations and individuals to be vetted for links to terrorism before awarding contracts, grants, cooperative agreements, and other types of assistance like training or in-kind assistance. The criteria considers dollar value for cumulative awards, award types, and how much time has passed since the organization was last vetted to determine whether vetting is required.

In response to deficiencies identified by the U.S. Government Accountability Office[1] and USAID/Office of Inspector General,[2] USAID/West Bank and Gaza deployed the Partner Vetting System (PVS) in 2006.

[1] GAO-06-1062R, *West Bank and Gaza Antiterrorism Procedures*, September 29, 2006.
[2] "Audit of the Adequacy of USAID's Antiterrorism Vetting Procedures," Report No. 9-000-08-001-P, November 6, 2007.

Partner Vetting System Nongovernmental Organization Portal

In June 2012 USAID/West Bank and Gaza launched the Partner Vetting System Nongovernmental Organization (PVS NGO) Portal, a Web-based application that allows implementing partners to prepare and submit vetting requests. Before this portal was launched, mission staff received vetting requests from implementing partners via e-mail and manually entered the data into the system. The purpose of the portal was to reduce the amount of time mission employees spent entering these data. However, they still have to enter data on all vetting requests from partners that do not have access to the portal, as well as all subawards, and to track the cumulative $25,000 threshold for contracts—a requirement of Mission Order 21.

USAID/Office of Security owns both PVS and the PVS NGO portal.

Geo-Management Information System

In 2002 USAID/West Bank and Gaza hired Systematics Inc., a local information technology (IT) contracting firm, to develop the Geo-Management Information System (Geo-MIS). The mission owns Geo-MIS, and the system administrators oversee account management and other business functions. This system helps mission employees who often cannot perform site visits because of security concerns. In addition, the system serves as a source of information for the mission's reporting requirements—requests for data calls from USAID/Washington and quarterly and annual reporting. Information from Geo-MIS also serves as a source for public outreach and information dissemination to Palestinian Authority officials and key stakeholders such as USAID/Washington.

In May 2012 the mission awarded Systematics another contract to upgrade Geo-MIS. From the system's inception in 2002 through September 30, 2013, the mission has obligated a total of $1.5 million and disbursed $1.4 million to Systematics for design and IT support services.

The Regional Inspector General/Cairo (RIG/Cairo) conducted this audit as part of its fiscal year 2013 audit plan. The objective was to determine whether USAID/West Bank and Gaza implemented minimum security controls to protect the confidentiality, integrity, and availability of these three systems, in compliance with NIST.

Our audit results showed that the owners of the systems have implemented some security controls—listed below—to comply with NIST's security requirements.

- The mission provided periodic training to all account users on how to use the three information systems.

- The Office of Security prepared risk assessment policies and procedures for PVS and the PVS NGO Portal.

- The Office of Security properly conducted security categorization for PVS and the portal.

- The Office of Security implemented contingency planning policies and procedures for PVS and the portal.

- The Office of Security completed security assessments on PVS and the portal.

- The mission developed a contingency plan for Geo-MIS.

- The mission developed policies and procedures for Geo-MIS usage.

Nonetheless, the audit testing found that the following security controls needed improvement.

- Information systems' risk assessments were not completed (page 7). The mission did not conduct a risk assessment for Geo-MIS, and the Office of Security had not conducted a periodic review of the PVS NGO Portal risk assessment since 2011.

- Information systems' security assessments were not completed (page 9). Because the mission did not conduct security assessments and certification and accreditation processes on Geo-MIS, the system did not have the security authorization from the chief information security officer to operate.

- The mission did not complete a security plan for Geo-MIS (page 10).

- Contingency plan controls were not implemented fully (page 11). While the mission relied on Agency policies and procedures for contingency planning, its contingency plan for Geo-MIS did not comply with requirements like testing the plan and establishing an alternate process site. Similarly, the Office of Security did not conduct periodic contingency plan testing and establish an alternate processing site for the portal.

- Some access controls were ineffective (page 14). Controls for Geo-MIS were weak in policies and procedures, account management, separation of duties, unsuccessful log-on attempts, system-use notification, and session lock.[3] Controls in account management of PVS and the portal were weak, and access controls like separation of duties and least privileges were ineffective in PVS.

- Identification and authentication controls were not implemented fully (page 19). The mission did not have comprehensive policies and procedures for identifying and authenticating Geo-MIS users. The portal and Geo-MIS also have weaknesses in password management of user accounts.

- Geo-MIS's session authenticity control was ineffective (page 21). The system was not secure in transmitting data after users first logged on.

- Some portal input controls were not implemented fully (page 23). Anomalies in the system did not allow users to enter required information for vetting and save changes to correct input errors.

- Users did not certify data in Geo-MIS consistently (page 23). Assistance officer's and contracting officer's representatives (AORs/CORs) did not certify data reported by the implementing partners consistently, as required.

[3] A session lock automatically prevents disclosure of information by locking an application or an employee workstation after a predetermined period of inactivity. The workstation or application remains locked until the user reestablishes access using appropriate identification and authentication procedures.

To help improve the efficiency and effectiveness of the mission's information systems, this audit recommends that:

1. The mission implement written risk assessment procedures documenting roles and responsibilities of mission staff, and periodic review for Geo-MIS in accordance with NIST SP 800-53 (page 8).

2. The mission document a risk assessment of Geo-MIS in accordance with FIPS 199 and NIST SP 800-30, and categorize Geo-MIS as a low-, moderate-, or high-risk system (page 8).

3. The Office of Security conduct and document periodic risk assessments for the PVS NGO Portal to comply with the guidance of NIST SP 800-53 (page 8).

4. The mission prepare a written security assessment of Geo-MIS in accordance with NIST SP 800-53 (page 10).

5. Based on the results of the security assessment, the mission should document its plan of action and milestones for Geo-MIS in accordance with NIST SP 800-53 (page 10).

6. USAID/Office of Security update the portal plan of action and milestones to include estimated completion dates for the milestones (page 10).

7. Once the estimated completion dates are in the portal's plan of action and milestones, the Office of Security implement procedures to conduct periodic reviews and document updates of actions taken to address the security control weakness by the completion dates (page 10).

8. The mission obtain a certified authorization to operate Geo-MIS from the Agency's chief information security officer in accordance with Automated Directives System (ADS) 545 (page 10).

9. The mission implement a security plan in accordance with NIST SPs 800-53 and 800-18 for Geo-MIS (page 11).

10. The mission implement comprehensive contingency plan procedures in accordance with NIST SPs 800-53 and 800-34 for its information systems including Geo-MIS (page 13).

11. Upon completion of the Geo-MIS contingency plan, the mission should implement procedures to test its plan annually and update the contingency plan as needed based on the results (page 13).

12. The Office of Security review the PVS NGO Portal contingency plan and make corrections as necessary in accordance with NIST SP 800-53 (page 13).

13. The Office of Security complete its annual testing of PVS and the portal, and update the contingency plans based on the results (page 14).

14. The mission coordinate with the Office of Security to identify an alternate processing site for the portal and incorporate the site into its contingency plan (page 14).

15. The mission include recovery of the information systems once normal operations return in its Geo-MIS contingency plan (page 14).

16. The mission modify Geo-MIS to include a transaction recovery system, such as transaction rollback[4] or transaction journaling,[5] to help recover the database in the event of a failure, as required by NIST SP 800-53 (page 14).

17. The mission modify its Geo-MIS access control procedures and include the topics required by NIST 800-53 (page 15).

18. The mission implement procedures (1) defining and requiring periodic review of user accounts and roles, and (2) deactivating invalid user accounts within Geo-MIS, PVS, and the PVS NGO Portal as required by NIST 800-53 (page 15).

19. The Office of Security incorporate audit trails for creation of user accounts, last user log-ons, role modifications, and disabling of user accounts for PVS as required by NIST SP 800-53, and give the mission access to the system's audit trails (page 15).

20. The mission incorporate audit trails for creation of user accounts, last user log-ons, role modifications, and disabling of user accounts to Geo-MIS as required by NIST SP 800-53 (page 16).

21. The mission implement procedures requiring written access requests for all authorized PVS and Geo-MIS users (page 16).

22. The mission (1) review and document the review results on roles assigned to GEO-MIS and PVS administrators, and (2) correct any separation of duties weaknesses noted, or document reasons for not correcting them (page 16).

23. The mission review and document the results of the review on users with system administrator rights and other privileged roles in PVS and remove these roles as needed to enforce least privilege (page 17).

24. The mission document the acceptable number of user log-on attempts before Geo-MIS user accounts are locked and incorporate this control into the Geo-MIS application (page 17).

25. The mission modify its Geo-MIS user notification to comply with NIST SP 800-53 (page 18).

26. The mission define its session lock criteria for Geo-MIS in management-approved procedures (page 18).

[4] A transaction rollback is an operation that returns the database to some previous state. Rollbacks are important for database integrity because they mean that the database can be restored even after erroneous operations are performed. They are also important for recovering from database server crashes; by rolling back transactions at the time of the crash, the database can be restored to a consistent state.

[5] A transaction journal is a history of actions executed by a database management system, and it is used to recover a database if a system crashes. Physically, a transaction journal is a file of updates done to the database, stored in stable space.

27. The mission modify Geo-MIS to prevent the display of data once the system locks a session (page 18).

28. The mission provide training to the system administrators of PVS, the PVS NGO Portal, and Geo-MIS on information system security and security requirements for federal information systems (page 19).

29. The mission implement a comprehensive identification and authentication policy and procedures for Geo-MIS to comply with the guidance of NIST SP 800-53 (page 20).

30. Following the implementation of the identification and authentication policy and procedures for Geo-MIS, the mission should conduct periodic reviews and document the review results to comply with the guidance of NIST SP 800-53 (page 20).

31. The mission incorporate authenticator management controls in Geo-MIS to enforce (1) minimum password complexity, (2) minimum number of changed characters when new passwords are created, (3) encrypted representations of passwords for storage and transmission, (4) password minimum and maximum lifetime restrictions, (5) rules governing the recycling of passwords, and (6) the use of a temporary password for system log-ons with an immediate change to a permanent password, in compliance with NIST SP 800-53 (page 21).

32. The Office of Security incorporate authenticator management control in the portal to enforce minimum password lifetime parameters for user accounts to comply with NIST SP 800-53 (page 21).

33. The mission implement controls in Geo-MIS so the system does not retain user log-ons once it ends a session (page 22).

34. The mission use a secure session for transmitting data from its implementing partners (page 22).

35. The mission, in coordination with the Office of Security, implement necessary changes to the portal to eliminate restrictions on age limits in the birth date fields in the partner information form and to allow changes made to be reflected in the form (page 23).

36. The mission review and document the frequency and level of certification required by the CORs and AORs to perform in Geo-MIS (page 25).

37. The mission implement a policy to periodically validate CORs' and AORs' compliance with Geo-MIS certification requirements (page 25).

The details of our audit findings are in the sections below. Appendix I contains information on the audit scope and methodology. Our evaluation of management comments is on page 26, and management comments, excluding attachments are included in Appendix II.

AUDIT FINDINGS

Information Systems' Risk Assessments Were Not Completed

FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems" includes standards all federal agencies use to categorize information systems maintained by or on behalf of each agency. The objective is to provide appropriate levels of information security controls according to a range of risk levels. Agencies can then classify their systems under three risk categories: low, moderate, or high.

To help federal agencies to comply with the regulations, NIST provided SP 800-30, "Guide for Conducting Risk Assessments," which explains the process for developing a system risk assessment. This guide gives organizations flexibility on how to conduct the required risk assessments and apply guidance to address the various organizational needs so the assessment activities are integrated into broader organizational risk management processes.

NIST also published SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," which gives guidance on the types of controls agencies need to implement to address risks identified from the assessments. The guidance categorizes security controls into 18 "families," including one on risk assessment. Within the risk assessment family, there are five controls. The following table summarizes the results of three selected risk assessment controls tested.

Table 1. Risk Assessment Controls Tested and Results

		Control Met		
Risk Assessment (RA) Control Number	**Description**	**Geo-MIS**	**PVS**	**PVS NGO Portal**
RA-1	Risk Assessment Policy and Procedures	No	Yes	Yes
RA-2	Security Categorization	No	N/A*	Yes
RA-3	Risk Assessment	No	Yes	Partial

* We did not test this control because the plan of action and milestones was tested in Washington, D.C.

While PVS met the minimum controls, Geo-MIS met none and the PVS NGO Portal met two, as discussed below.

RA-1 Risk Assessment Policy and Procedures. NIST SP 800-53 requires agencies to implement written risk assessment procedures documenting roles, responsibilities, coordination among organizational entities, and compliance. Furthermore, NIST requires periodic reviews and updates of the procedures.

The mission did not have written procedures in place covering a risk assessment process for Geo-MIS. According to the information system security officer, the mission followed the risk assessment policy and procedures from ADS 545 for PVS and the portal. However, it did not perform any risk assessments on Geo-MIS, as required by NIST 800-53 and ADS 545.

RA-2 Security Categorization and RA-3 Risk Assessment. In accordance to NIST SP 800-53, an agency should categorize its information and information system in accordance with applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance, and it should then document the security categorization results (including supporting rationale) in the security plan for the information system.

To accomplish the security categorization, the mission should use a risk assessment process to determine how to categorize information systems like Geo-MIS. The assessment should consider and address the likelihood and impact of potential damage from unauthorized access, use, disruption, modification, or destruction of the information system as well as its data. Mission management should review and approve the risk categorization. It should also be reviewed periodically to reflect any significant changes to the system.

While USAID's chief information officer allowed the use of Geo-MIS, neither he nor the mission had a documented risk assessment categorizing the system as low, moderate, or high. For the PVS NGO Portal, the last periodic review of the risk assessment was done in 2011.

The mission did not perform an assessment because officials said they assumed that the chief information officer's approval to use the system sufficed and no additional assessments were required. Furthermore, the mission's staff generally was unaware of how the federal security requirements for information systems should be applied.

Regardless of the approval process, each federal information system must be assessed. By not having a risk assessment and classification of Geo-MIS, the mission cannot be sure it is fully compliant with the minimum baseline security controls required by NIST SP 800-53. In fact, as discussed in the findings below, for Geo-MIS several minimum security controls either did not exist or needed improvement. These controls—based on the assessed level of risk—protect organizational operations and assets, individuals, and other organizations from threats including natural disasters, structural failures, and intentional and unintentional human errors. We therefore make the following recommendations.

Recommendation 1. *We recommend that USAID/West Bank and Gaza implement written risk assessment procedures documenting roles and responsibilities of mission staff, and periodic review for the Geo-Management Information System in accordance with National Institute for Standards and Technology Special Publication 800-53.*

Recommendation 2. *We recommend that USAID/West Banks and Gaza document a risk assessment of the Geo-Management Information System in accordance with federal information processing standard 199 and National Institute for Standards and Technology Special Publication 800-30, and categorize the system as low-, moderate-, or high-risk.*

Recommendation 3. *We recommend that USAID/Office of Security implement procedures to conduct and document periodic risk assessments for the Partner Vetting System Nongovernmental Organization Portal to comply with the guidance of National Institute for Standards and Technology Special Publication 800-53.*

Information Systems' Security Assessments Were Not Completed

FIPS 200 specifies minimum-security requirements for information systems supporting federal executive agencies and a risk-based process for selecting the security controls necessary to satisfy minimum-security requirements. NIST SP 800-53 has seven minimum security assessment controls required for moderate-risk systems. Table 2 summarizes the controls tested and the audit results.

Table 2. Security Assessment and Authorization Controls Tested and Results (Audited)

		Control Met		
Security Assessment Control Number	**Description**	**Geo-MIS**	**PVS**	**PVS NGO Portal**
CA-2	Security Assessment	No	Yes	Yes
CA-5	Plan of Action and Milestones	No	N/A*	Partial
CA-6	Security Authorization	No	N/A**	Yes

* We did not test this control because the plan of action and milestones was tested in Washington, D.C.

** We did not test this control because security authorization was tested in Washington, D.C.

While the mission had authorization to use each information system, it did not prepare a security assessment for Geo-MIS, and the PVS NGO Portal did not have an updated plan of action and milestones as described below.

CA-2 Security Assessment. NIST 800-53 requires agencies to develop a security assessment plan that describes the scope with security controls assessed; assessment procedures that would be used to determine security control effectiveness; team and their roles and responsibilities. In addition, agencies should assess the security controls of the information system periodically, document the results, and report them to the designated officials. While PVS and the portal have completed security assessments, Geo-MIS did not.

CA-5 Plan of Action and Milestones. NIST 800-53 requires agencies to develop a plan of action and milestones for each information system documenting the planned remedial actions to correct weaknesses or deficiencies identified during the security controls assessment and to reduce or eliminate known vulnerabilities in the system. These requirements state that system owners should update the plan of action and milestones periodically, based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

Since there was no security assessment for Geo-MIS, a plan of action and milestones to correct identified weaknesses does not exist. While a plan of action and milestones exists to correct identified weakness from a previous assessment of the PVS NGO Portal, it is not dated and does not contain milestone completion dates. According to an Agency representative, the plan was completed in December 2011; however, as of October 2013, there was no update on the implementation of the corrective actions.

CA-6 Security Authorization. NIST SP 800-53 requires agencies to appoint a senior-level executive or manager to (1) be the authorizing official for the information system, (2) make sure this official authorizes the system before it starts operating, and (3) update the security authorization periodically. ADS 545 designates the Agency's chief information security officer

(CISO) as the person responsible for providing a certified authorization to operate information systems.

The PVS NGO Portal has a documented certification. However, the mission relied on the permission it received to use Geo-MIS and did not obtain a certified authorization to use the system. While the mission has permission to use Geo-MIS, the Agency's CISO still requires the mission to follow the Agency's certification and accreditation plan outlined in ADS 545, which includes a formal security authorization.

An information security assessment is important because it determines how effectively a system meets specific security objectives. Similarly, security control assessments determine whether controls are being implemented correctly, operating as intended, and producing the desired outcome. These assessments document a plan of action and milestones, including remedial actions to correct issues noted during the security controls assessment and to reduce vulnerabilities in the system. In turn, action plans help monitor progress made on reducing system vulnerabilities through the implementation of required security controls. Therefore, we make the following recommendations.

Recommendation 4. *We recommend that USAID/West Bank and Gaza prepare a written security assessment of the Geo-Management Information System in accordance with National Institute for Standards and Technology Special Publication 800-53.*

Recommendation 5. *Based on the results of the security assessment, we recommend that USAID/West Bank and Gaza document its plan of action and milestones for the Geo-Management Information System in accordance with National Institute for Standards and Technology Special Publication 800-53.*

Recommendation 6*. We recommend that USAID/Office of Security update the Partner Vetting System Nongovernmental Portal plan of action and milestones to include estimated completion dates for its established milestones.*

Recommendation 7. *Once the estimated completion dates are in the Partner Vetting System Nongovernmental Portal's plan of action and milestones, we recommend that USAID/Office of Security conduct periodic reviews and document updates of actions taken to address any security control weaknesses by the completion dates.*

Recommendation 8*. We recommend that USAID/West Bank and Gaza obtain a certified authorization to operate the Geo-Management Information System from the Agency's Chief Information Security Officer in accordance with Automated Directives System 545.*

Geo-Management Information System Did Not Have Security Plan

NIST SP 880-53 lays out four minimum-security planning controls federal information systems must comply with. According to that, the mission—as the system owner—was required to develop a security plan for Geo-MIS covering, in part:

- The security categorization of the information system including supporting rationale.

- The operational environment for the information system and relationships with or connections to other information systems.

- An overview of the security requirements for the system.

- The security controls in place or planned for meeting those requirements.

The mission also was required to have the plan formally approved by management, and distributed and reviewed based on a predefined schedule.

NIST SP 800-18, "Guide for Developing Security Plans for Federal Information Systems," gives agencies specific guidance to develop security plans. While PVS and the PVS NGO Portal met these minimum requirements, Geo-MIS did not.

The mission did not have a security plan for Geo-MIS because it did not conduct a formal risk assessment (discussed in the previous finding). Furthermore, the mission employees in charge of the system were unaware of the U.S. Government regulations covering information system security controls.

A system security plan is important because it improves protection for information system resources. It provides an overview of system requirements and describes actual and planned controls. Finally, a plan documents management's due diligence by providing documentation that a planning process was followed that resulted in cost-effective controls. We therefore make the following recommendation.

Recommendation 9. *We recommend that USAID/West Bank and Gaza implement a security plan in accordance with National Institute for Standards and Technology Special Publications 800-53 and 800-18 for the Geo-Management Information System.*

Contingency Plan Controls Were Not Implemented Fully

NIST SP 800-34, "Contingency Planning Guide for Federal Information Systems" provides detailed guidance for developing contingency plans. NIST SP 800-53 lays out nine minimum contingency planning controls that federal information systems must comply with. The following table summarizes the results for five of nine contingency plan controls tested during fieldwork.

Table 3. Contingency Planning Controls Tested and Results (Audited)

		Control Met		
Contingency Plan Controls	**Description**	**Geo-MIS**	**PVS**	**PVS NGO Portal**
CP-1	Contingency Plan Policies and Procedures	Partial	Yes	Yes
CP-2	Contingency Plan	Partial	N/A*	Partial
CP-4	Contingency Plan Testing	No	Partial	Partial
CP-7	Alternate Processing Site	Yes	Yes	No
CP-10	Information System Recovery	No	Yes	Yes

* We did not test this control because contingency plan policies and procedures were tested in Washington, D.C.

While the mission relied on ADS 545.3.3.7, "Contingency Planning," to shape its contingency planning procedures, the audit identified shortcomings in several areas of the plan that are discussed below.

CP-2 Contingency Plan. NIST SP 800-53 requires agencies to develop a contingency plan covering five specific topics:

- Identifying business functions
- Providing recovery objectives, restoration priorities, and metrics
- Addressing contingency roles and responsibilities of assigned individuals with contact information
- Addressing the maintenance of essential missions and business functions despite an information system disruption, compromise, or failure
- Addressing eventual, full information system restoration without eliminating the security safeguards originally planned and implemented.

Management also is required to approve the contingency plan. Once it is approved, the mission should distribute the plan to appropriate personnel, have it reviewed and updated periodically, and communicate any updates to appropriate staff.

While there is a written Geo-MIS contingency plan, it lacks specificity. The plan is a one-page document that discusses issues such as the backup cycle and purchasing equipment in the event of a system failure. The plan lacks the five critical elements required by NIST SP 800-53. Furthermore, it does not have the requisite approval from management, and there is no evidence that it was distributed to required mission staff or that the plan was reviewed annually. Since the start of audit fieldwork, the mission has been in the process of making its plan compliant with NIST SP 800-53.

For the PVS NGO Portal, while there is a formal contingency plan covering the requisite topics, we could not determine whether the Office of Security has reviewed it periodically since September 2011.

CP-4 Contingency Plan Testing. NIST SP 800-53 requires agencies to test contingency plans periodically, review test results, and update plans based on results as needed. ADS 545.3.3.7 requires agencies to test contingency plans annually. For Geo-MIS, the mission could not provide documentation that it tested its plan. For PVS and the PVS NGO Portal, the mission provided supporting documentation for contingency plan tests performed in 2009 and 2011; however, none have been performed since.

CP-7 Alternate Processing Site. NIST SP 800-53 requires agencies to have an alternate processing site available within a specified period for business systems once primary systems become unavailable. The site should have sufficient supplies and equipment and be separate from the primary site. According to the system's contingency plan, all operations will be moved to the alternate site when the plan is activated.

While the mission and Office of Security have identified alternate processing sites for Geo-MIS and PVS, they have not for the PVS NGO Portal. According to the mission, if the portal goes down, it will revert to a manual process. However, according to NIST, the mission or Office of Security should have an alternate processing site for moderate-risk systems like the portal.

CP-10 Information System Recovery. NIST SP 800-53 requires agencies to provide for the recovery and reconstruction of the information system to a known state after a disruption, compromise, or failure. Furthermore, the information system should implement a transaction recovery system for systems that are transaction-based like database management systems. Examples of mechanisms supporting transaction recovery include transaction rollback and transaction journaling. PVS and the PVS NGO Portal contingency plans provide for the recovery of the information systems once normal operations return, and the database management systems for them provide for transaction recovery. However, the Geo-MIS contingency plan and the database do not meet these requirements.

The mission did not develop the contingency controls for Geo-MIS properly for a variety of reasons. First, a formal risk assessment that would have identified the minimum contingency planning controls was not completed, as discussed in the previous finding. Second, the mission employees in charge of Geo-MIS said they were unaware of the U.S. Government regulations covering these controls. Finally, because the program office did not involve the mission's information technology staff in the security controls aspect of the system, the Geo-MIS contingency plan did not fully address the required steps under the guidance.

The PVS project manager said staff changes at USAID and at the external contracting company supporting USAID/Washington were some possible reasons for not performing annual tests of PVS and the portal. He recently assumed responsibility for the system and could not explain why it was not tested annually.

Contingency planning is an important control because it allows the mission to continue operations in the event of an emergency. It is critical that identified services provided by the mission's information systems are able to operate effectively without excessive interruption. Contingency planning supports this requirement by establishing thorough plans, procedures, and technical measures that enable a system to be recovered as quickly and effectively as possible after a service disruption. Contingency planning is unique to each system, providing preventive measures, recovery strategies, and technical considerations appropriate to the information system's risk, confidentiality, integrity, and availability requirements. Furthermore, annual review and testing of contingency plans provides some level of assurance that the plan is still meeting the mission's needs and has been implemented successfully.

Recommendation 10. *We recommend that USAID/West Bank and Gaza implement comprehensive contingency plan procedures in accordance with National Institute for Standards and Technology Special Publications 800-53 and 800-34 for its information systems including the Geo-Management Information System.*

Recommendation 11. *Upon completion of the Geo-Management Information System contingency plan, we recommend that USAID/West Bank and Gaza implement procedures to test its plan annually and update the contingency plan as needed based on the results.*

Recommendation 12. *We recommend that USAID/Office of Security review the Partner Vetting System Nongovernmental Organization Portal contingency plan and make*

corrections as necessary in accordance with National Institute for Standards and Technology Special Publication 800-53.

Recommendation 13. *We recommend that USAID/Office of Security complete its annual testing of the Partner Vetting System and the Partner Vetting System Nongovernmental Organization Portal, and update the contingency plans based on the results.*

Recommendation 14. *We recommend that USAID/West Bank and Gaza coordinate with USAID/Office of Security to identify an alternate processing site for the Partner Vetting System Nongovernmental Organization Portal and incorporate the site into its contingency plan.*

Recommendation 15*. We recommend that USAID/West Bank and Gaza include recovery of the information systems once normal operations return in its Geo-Management Information System contingency plan.*

Recommendation 16. *We recommend that USAID/West Bank and Gaza modify the Geo-Management Information System to include a transaction recovery system, such as transaction rollback or transaction journaling, to assist in the recovery of the database in the event of a failure, as required by National Institute for Standards and Technology Special Publication 800-53.*

Some Access Controls Were Ineffective

According to NIST SP 800-53, agencies must limit information system access to authorized users, processes acting on behalf of authorized users, or devices such as other information systems. Access should be limited also to the types of transactions and functions that authorized users are permitted to perform. NIST SP 800-53 includes 18 access controls for federal information systems compliance. The following table summarizes a list of the specific controls tested during the audit and the results.

Table 4. Access Controls Tested and Results (Audited)

		Control Met		
Access Control	**Description**	**Geo-MIS**	**PVS**	**PVS NGO Portal**
AC-1	Access Control Policy and Procedures	Partial	Yes	Yes
AC-2	Account Management	Partial	Partial	Partial
AC-5	Separation of Duties	Partial	Partial	Yes
AC-6	Least Privilege	Yes	Partial	Yes
AC-7	Unsuccessful Log-on Attempts	No	Yes	Yes
AC-8	System Use Notification	Partial	Yes	Yes
AC-11	Session Lock	Partial	Yes	Yes

The mission requires corrective action in six Geo-MIS controls. For the PVS, corrective actions are required in three control areas, and for the PVS NGO Portal, one, described on the next page.

AC-1 Access Controls Policies and Procedures. NIST SP 800-53 requires agencies to implement written access control procedures documenting roles, responsibilities, management commitment, and coordination among organizational entities, access controls, and compliance. Furthermore, NIST requires periodic reviews and updates of the procedures.

The mission implemented written procedures for Geo-MIS. However, there is no evidence that management reviewed and documented approval of the procedures. Furthermore, the procedures do not define certain access controls such as the periodic review of the procedure itself and how this review is to be documented. The written procedures do not cover mission-defined access control policies such as time limits for session lock and the number of unsuccessful log-on attempts before the system locks a user account.

Recommendation 17. *We recommend that USAID/West Bank and Gaza modify its Geo-Management Information System access control procedures and include the topics required by National Institute for Standards and Technology Special Publication 800-53.*

AC-2 Account Management. NIST SP 800-53 requires 15 specific minimum control activities for account management, including (1) assigning account managers for systems, (2) establishing conditions for group membership, (3) requiring management approvals for requests to create information system accounts, (4) creating, enabling, modifying, disabling, and removing accounts in accordance with established procedures, and (5) monitoring the use of accounts. The mission did not have controls in the following areas.

- Periodic review of accounts. There was no evidence supporting the reviews of user accounts for Geo-MIS, PVS, and the PVS NGO Portal. As a result, invalid accounts that should have been disabled remained active. Account verification of users at the mission and at 16 implementing partners showed that 4 Geo-MIS and 19 portal user accounts were no longer valid and should have been disabled.

- Audit trails for account creation, last log-ons, role modification, and disabling of user accounts. While PVS has an audit trail feature that keeps a record of when an account is created, modified, and disabled in the PVS NGO Portal, it does not track when PVS user accounts are created, modified, and disabled. Geo-MIS has an audit trail feature for user account activities, but it does not keep a record of when user accounts are created, modified, and disabled. Geo-MIS also does not keep a record of the most recent log-ons.

- Records of access authorization. The PVS system administrator grants users access to PVS without a formal access request, and the Geo-MIS system administrator did not maintain authorization and records of access authorization consistently to Geo-MIS.

Recommendation 18. *We recommend that USAID/West Bank and Gaza implement procedures (1) defining and requiring periodic review of user accounts and roles, and (2) deactivating invalid user accounts within the Geo-Management Information System, Partner Vetting System, and Partner Vetting System Nongovernmental Organization Portal as required by National Institute for Standards and Technology Special Publication 800-53.*

Recommendation 19. *We recommend that USAID/Office of Security incorporate audit trails for creation of user accounts, last user log-ons, role modifications, and disabling of user accounts to the Partner Vetting System as required by National Institute for*

Standards and Technology Special Publication 800-53, and give USAID/West Bank and Gaza access to the audit trails.

Recommendation 20. *We recommend that USAID/West Bank and Gaza incorporate audit trails for creation of user accounts, last user log-ons, role modifications, and disabling of user accounts to the Geo-Management Information System as required by National Institute for Standards and Technology Special Publication 800-53.*

Recommendation 21. *We recommend that USAID/West Bank and Gaza implement procedures requiring written access requests for all authorized Partner Vetting System and Geo-Management Information System users.*

AC-5 Separation of Duties. NIST SP 800-53 requires agencies to document the separation of duties within a system and to use the system's access controls to enforce this separation. Contrary to the guidance, the roles assigned for AORs and CORs in Geo-MIS allowed them to edit data entered by the implementing partners. According to the mission's program office management and Geo-MIS's system administrator, final reported data are a collaborative product between AORs/CORs and partners. Therefore, one of the system requirements allows AORs/CORs to edit data entered by the partner.

While this was an intentional decision on the part of mission management, the system did not track the justification for edits done by the AORs/CORs. Further, the role of AORs/CORs was to review and certify implementer partner data and not enter information on behalf of the partner. Therefore, it is vital that major changes be supported by written justification and communicated to the partners for lessons learned.

Additionally, the review of account user roles also identified a lack of separation of duties in both Geo-MIS and PVS, which allowed system administrators to perform other business functions in the systems such as editing and processing data. For example, Geo-MIS system administrators could modify data in the system and update various tables visible and not visible to regular users as well as account managers. Similarly, PVS system administrators at the mission not only managed user accounts but also performed other data processing tasks.

Recommendation 22. *We recommend USAID/West Bank and Gaza (1) review and document the review results on roles assigned to Geo-Management Information System and Partner Vetting System administrators, and (2) correct any separation of duties weaknesses noted, or document reasons for not correcting noted weaknesses.*

AC-6 Least Privilege. NIST SP 800-53 requires that users be assigned roles only within a system that is required to perform approved tasks. The audit analyzed user privileges and found that 7 of the 10 privileged PVS user accounts were still assigned with data processor and coordinator roles after the portal was implemented.

Before the portal's launch, the roles of data processor and coordinator allowed mission staff to enter vetting information from the partner information form (PIF) into PVS. Now partners prepare electronic forms and transmit them through the PVS NGO Portal. According to the mission, about 80 percent of the partners use the portal, eliminating most of mission's burdensome task of entering data. As a result, the number of manual PIFs that mission employees must enter into PVS has decreased greatly.

However, the mission did not adjust the number of user accounts with data processor and coordinator roles to reflect this change. Mission officials said they did not because the users still need the assigned roles for data entry in PVS for subaward reporting.

Furthermore, four of these privileged users had a system administrator role plus other functional roles that may be more than they need for their jobs. Since there was no written justification for these additional roles, we question whether these system users actually need the additional roles to perform their work responsibilities.

> ***Recommendation 23.*** *We recommend that USAID/West Bank and Gaza review and document the results of the review on users with system administrator rights and other privileged roles in the Partner Vetting System, and remove these roles as needed to enforce least privilege.*

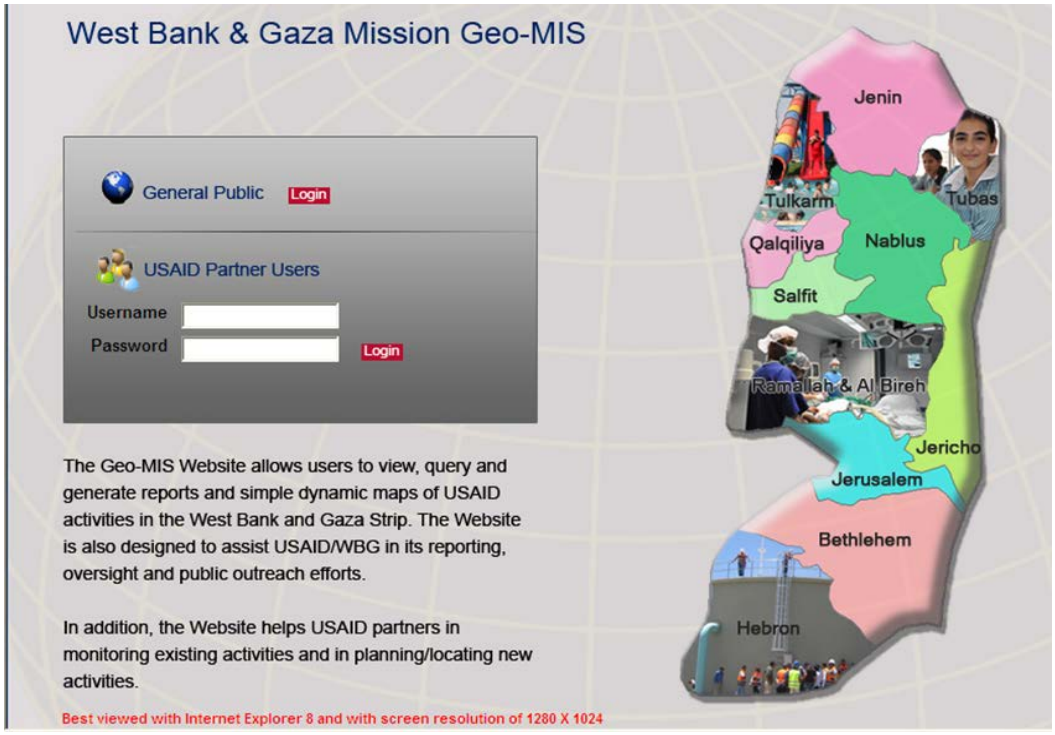
AC-7 Unsuccessful Log-on Attempts. NIST SP 800-53 requires that the system automatically lock an account for a set period of time or until reset by an administrator after a predetermined number of unsuccessful attempts to log on. Testing of Geo-MIS and interviews with system users showed that the system does not lock user accounts after a predetermined number of unsuccessful log-on attempts. Furthermore, the current written Geo-MIS procedures do not define how many log-on attempts are acceptable, which contributes to weaknesses in the system.

> ***Recommendation 24.*** *We recommend that USAID/West Bank and Gaza document the acceptable number of user log-on attempts before a Geo-Management Information System user account is locked and incorporate this control into the Geo-Management Information System application.*

AC-8 System Use Notification. NIST SP 800-53 requires that the system display a "system use notification when a user accesses a system." This notification must include a statement that the user is accessing a U.S. Government System; the system may be monitored and subject to audit; unauthorized use is prohibited, and system users consent to monitoring of their activities. Furthermore, the notification is to remain in place until the user takes explicit action to close the message. Finally, for systems open to the public, there are two additional requirements: display of system use information before granting further access and a description of what constitutes authorized use.

Geo-MIS's use notification does not meet these requirements. For example, there is no notification to users that they are accessing a U.S. Government information system and their activities in the system are subjected to monitoring and audit, as seen in the screen print of the Geo-MIS log-on screen on the next page.

Screen Print of the Geo-MIS Web Site



The system use notification that anyone accessing Geo-MIS sees does not meet certain requirements. (Print obtained by RIG/Cairo during fieldwork)

Recommendation 25. *We recommend that USAID/West Bank and Gaza modify its Geo-Management Information System user notification to comply with National Institute for Standards and Technology Special Publication 800-53.*

AC-11 Session Lock. NIST SP 800-53 requires that an information system prevent further access to it by initiating a session lock after a period of time of inactivity defined by the management. Once the session is locked, the system should conceal information displayed previously.

Geo-MIS does have a session lock after 60 minutes of inactivity, but there was no evidence within the written procedures that management specified that amount of time. Once the session lock was active, it did not hide the previously displayed data. During testing, a user was able to see the displayed data and change data on the screen, but could not save the changes. In fact, the system did not notify the user that the lock was active until the user tried to save changes.

Recommendation 26. *We recommend that USAID/West Bank and Gaza define and document its session lock criteria for the Geo-Management Information System in management-approved procedures.*

Recommendation 27. *We recommend USAID/West Bank and Gaza modify the Geo-Management Information System to prevent the display of data once the system locks the session.*

There were various causes for identified weaknesses in the selected access controls tested. For example, the primary cause for not getting a system use notification within Geo-MIS is the lack

of a risk assessment categorizing Geo-MIS and, in turn, establishing the minimum security baselines required. The lack of a written Geo-MIS security plan (as discussed in the previous findings) could have identified these weaknesses; therefore not having such a plan contributed to the lack of access control restrictions.

The Geo-MIS system administrator did not have any specialized training or experience in system security. One of that administrator's responsibilities was to protect information and maintain security protocols in collaboration with the mission's systems administrator. However, the mission's IT manager said his team—with knowledge of system security— was responsible for managing only the system server; they did not collaborate much on system security with the Geo-MIS administrator. In addition, the system administrator assigned to PVS and the PVS NGO Portal controls did not have enough system security training and experience to be responsible for securing the system. She said she felt unprepared to be responsible for the access controls.

Access controls are important because they limit who has the ability to see, edit, and use the data within systems. They also prevent the disclosure of sensitive information such as the GPS coordinates of activities being implemented by the mission and its partners, which could pose an unnecessary security risk. Finally, access controls also prevent unauthorized changes to data, both intentional and unintentional.

To address the system administrators' lack of information system security training and knowledge of security requirements on federal information systems, we make the following recommendation.

> ***Recommendation 28.*** *We recommend that USAID/West Bank and Gaza provide training to the system administrators of the Partner Vetting System, Partner Vetting System Nongovernmental Organization Portal and Geo-Management Information System on information system security and security requirements for federal information systems.*

Identification and Authentication Controls Were Not Implemented Fully

NIST SP 800-53 lays out eight minimum identification and authorization controls that federal information systems must comply with. However, selected identification and authentication controls tested for Geo-MIS and the PVS NGO Portal need improvement. The following table summarizes the controls tested during the audit and testing results.

Table 5. Identification and Authentication Controls Tested and Results (Audited)

		Control Met		
Access Control	**Description**	**Geo-MIS**	**PVS**	**PVS NGO Portal**
IA-1	Identification and Authorization Policies and Procedures	Partial	Yes	Yes
IA-5	Authenticator Management	No	Yes	Partial

IA-1 Identification and Authorization Policies and Procedures. NIST SP 800-53 requires that agencies establish and implement identification and authentication policies and procedures. Further, organizations must review and update those policies and procedures periodically.

While the mission has some procedures for Geo-MIS in place, it does not have evidence of management approval when establishing user accounts and defining user roles. The system administrator said the access control policy is updated continuously with new changes. However, the document does not include dates for the updates or approvals from mission management. Although the document addressed some basic requirements for access authorization for accounts and roles, it did not provide comprehensive guidance on the policies and procedures for password management.

> ***Recommendation 29.*** *We recommend that USAID/West Bank and Gaza implement a comprehensive identification and authentication policy and procedures for the Geo-Management Information System to comply with the guidance of National Institute for Standards and Technology Special Publication 800-53.*
>
> ***Recommendation 30.*** *Following the implementation of the identification and authentication policy and procedures for the Geo-Management Information System, we recommend that USAID/West Bank and Gaza implement procedures to conduct periodic reviews and document the review results to comply with the guidance of National Institute for Standards and Technology Special Publication 800-53.*

IA-5 Authenticator Management. NIST SP 800-53 requires agencies to manage information system authenticators like passwords, tokens, biometrics, and key cards. Some of the basic controls include:

- Minimum password complexity
- Minimum number of changed characters when creating new passwords
- Encryption of passwords for storage and transmission
- Use of a temporary password for system log-ons with an immediate change to a permanent password
- Minimum and maximum lifetime restrictions and reuse conditions for passwords
- Changing or refreshing passwords periodically.

Contrary to these requirements, the Geo-MIS system administrator reported manually generating passwords for each user account and e-mailing them to the user. He was the only person who could change the password. Fieldwork confirmed that 15 of 21 Geo-MIS account users (71 percent) have no option within the system to change their passwords, and most still have their originally assigned passwords. Further, Geo-MIS does not generate temporary passwords and does not require users to create a permanent password at initial log-on. The current passwords issued did not conform to any mission-established minimum complexity requirement for passwords.

The identification and authentication control weaknesses in Geo-MIS occurred because the system administrator did not receive any specialized training in system security and was not familiar with regulations for federal information systems. Compounding this problem, the mission IT staff was not involved with the program office in system implementation and administration. Another contributing factor is the lack of a security plan—as described in the previous finding—that could have found some of these identification and authentication requirements.

As for the PVS NGO Portal, account users were not required to change their passwords periodically. Testing during fieldwork confirmed that 14 of 35 users (40 percent) had not changed their original passwords, while the remaining users either forgot their passwords or were locked out due to inactivity. Although the security plan states that the USAID/Office of Security uses controls from AIDNet's Active Directory[6] to enforce minimum password lifetime parameters, the testing results showed otherwise. There is no requirement for users to change their passwords periodically—unlike AIDNet's requirement to change passwords every 90 days. Most portal users still use the original passwords they created after changing from the temporary ones the system generated. The results of the portal risk assessment showed this issue as a weakness; however, no corrective action was taken to address the risk.

Because of weak controls in identification and authentication in information systems, data in PVS, PVS NGO Portal, and Geo-MIS are at risk for unauthorized access that could result in data leaks, damaging mission development efforts and the Agency's reputation in the region.

> ***Recommendation 31.*** *We recommend that USAID/West Bank and Gaza incorporate authenticator management controls in the Geo-Management Information System to enforce (1) minimum password complexity, (2) minimum number of changed characters when new passwords are created, (3) encrypted representations of passwords for storage and transmission, (4) password minimum and maximum lifetime restrictions, (5) rules governing recycling of passwords, and (6) the use of a temporary password for system log-ons with an immediate change to a permanent password, in compliance with National Institute for Standards and Technology Special Publication 800-53.*
>
> ***Recommendation 32.*** *We recommend that USAID/Office of Security incorporate authenticator management control in the Partner Vetting System Nongovernmental Organization Portal to enforce minimum password lifetime parameters for user accounts to comply with National Institute for Standards and Technology Special Publication 800-53.*

Geo-Management Information System Session Authenticity Control Was Ineffective

NIST SP 800-53 lists 19 minimum session authenticity controls for moderate-risk federal information systems. One control requires that the information system protect the authenticity of the communications session. For example, the system should not retain user log-ons once the user terminates its activity with the system. Typically, organizations use Hyper Text Transport Protocol Secure (HTTPS) to transmit sensitive data securely over the Internet. HTTPS is similar

[6] The directory enforces account policies on password and account lock-out and local policies on audit policy, user rights assignment, and security options.

to Hyper Text Transfer Protocol, but uses a secure socket layer (SSL) for security purposes. SSL is a protocol for transmitting data over the Internet using encryption, and it allows passwords and user IDs to be transmitted securely. Once the system authenticates a user, it could revert to an unsecured connection, and this could allow data to be disclosed to unauthorized individuals.

While Geo-MIS used HTTPS to transmit user IDs and passwords, it did not maintain a secure connection once the users were authenticated. Furthermore, once a user terminated a session by closing the Internet browser screen, the browser continued to retain the user's ID and password. During our testing, we found that reopening the Internet browser and typing in the Web site for Geo-MIS brought up the Geo-MIS data, bypassing the log-on screen. Furthermore, testing also determined that once the log-on process was completed, data transfer between partners and the mission via Geo-MIS was not secured. The table below lists the control tested during the audit and the results.

Table 6. System Authenticity Control Tested and Results (Audited)

		Control Met		
Access Control	**Description**	**Geo-MIS**	**PVS**	**PVS NGO Portal**
SC-23	System Authenticity	No	Yes	Yes

The weaknesses occurred because the Geo-MIS system administrator and mission program office were not familiar with regulations and requirements for federal information systems. Furthermore, the mission's IT office—which oversaw the security of the mission's information systems—was not included in the implementation of the system; its only responsibility was to maintain the IT infrastructure. If the office had participated, the team there could have provided their expertise in information security to the system administrator to verify compliance with USAID regulations.

By switching from a secured to an unsecured connection after log-on, the mission exposes data to possible interception during transmission over the Internet. Furthermore, for implementing partners using wireless networks, the risk of having their data intercepted increases if secured protocols are not used to transmit data. This system weakness, in conjunction with not properly terminating the communications session, further exposes data such as GPS coordinates for project sites to unauthorized disclosure. Given the security situation within the West Bank and Gaza, this could expose mission and implementer project sites to unnecessary risks. We therefore are making the following recommendations.

Recommendation 33. *We recommend that USAID/West Bank and Gaza implement controls in the Geo-Management Information System so the system does not retain user log-ons after it terminates a communication session.*

Recommendation 34. *We recommend that USAID/West Bank and Gaza use a secure session for transmitting data from its implementing partners.*

Some Portal Input Controls Were Not Implemented Fully

According to Control Objectives for Information and Related Technology (COBIT) and *Application Controls: A Management Guide*, published by ISACA,[7], application input controls are used mainly to check the integrity of data entered into a business application, whether the data are entered directly by staff, remotely by a business partner, or through a Web-enabled application or interface. These controls are procedures used to verify, validate, and edit data, and to confirm that transactions are processed only once. Automated application controls can include predefined range limits, reasonableness tests, completeness checks to make sure all input fields are completed, and format checks to make sure data are treated consistently.

During our interviews with implementing partners, we found the following anomalies with the PVS NGO Portal application input controls.

- Birth Date Inputs. According to users (and verified by the mission), the system does not accept birth dates before 1940, and it rejects birth dates when the recipient being vetted is younger than 18 years old. To circumvent this problem, the partners are entering erroneous dates and then annotating the correct year in another field.

- Changes Not Saved. The portal does not retain changes made to correct erroneous information in PIFs once the forms are saved in the system. This anomaly occurs mainly in changes made to correct names of individuals and organizations. Because the corrections would not be reflected in the PIFs, users have to create a new PIF, which imposes a burden on the implementing partner.

The cause of these problems was rooted generally in the basic programming of the information system. If not corrected, they will continue to impose an unnecessary burden on the mission and the implementing partners because both need to be in constant communication with each other concerning corrections that should be done during data entry to the PIFs. To address improvement needed to the PVS NGO Portal, we are making the following recommendation.

> ***Recommendation 35.*** *We recommend that USAID/West Bank and Gaza, in coordination with USAID/Office of Security, implement necessary changes to the Partner Vetting System Nongovernmental Organization Portal to eliminate restrictions on age limits in the birth date fields in the Partner Information Form and allowing changes made to be reflected in the form.*

Users Did Not Certify Data in Geo-Management Information System Consistently

USAID ADS 203.3.11.1 states that performance data should be sufficiently precise to present a fair picture of performance, to enable management to make decisions, and to reflect stable, consistent data collection processes over time. High-quality data should meet five quality standards: validity, integrity, precision, reliability, and timeliness.

[7] COBIT is a framework created by ISACA for information technology management and governance. ISACA is an independent, nonprofit, global association works in the development, adoption, and use of globally accepted information systems.

IT industry best practices further emphasize the importance of reliable information. Application controls, which support information managed in IT systems, include manual and automated activities to make sure information in the system conforms to predetermined criteria.

As noted earlier, USAID West Bank and Gaza uses Geo-MIS to collect and organize performance data. This system has built-in data verification procedures, including COR/AOR certification of activities and indicator results. The Geo-MIS administrator manual states, "For the activities in a given program, the responsible COR (or AOR) is expected to review the monthly reports of uncertified activities, sequentially request each activity in the certification screen, make any additions and corrections to that activity record that are necessary, and finally certify the activity." This application control supports the goal of providing timely, accurate, and reliable information in Geo-MIS.

The mission's standard COR and AOR designation letters include requirements to be sure that the organization's information in Geo-MIS is accurate and to use the systems' validation and quality control tools.

Nonetheless, many CORs and AORs were not certifying project activities reported in Geo-MIS on time. As of November 13, 2013, the mission was managing 54 programs with 5,694 project activities in Geo-MIS. Each of these activities has an assigned COR or AOR responsible for program oversight. However, only 13 programs—24 percent—and 637 activities—11 percent—were certified in Geo-MIS by the responsible CORs or AORs.

One reason for the low rate was that some CORs and AORs said the system was confusing and not user-friendly. The mission implemented the certification feature of Geo-MIS in April 2013, and many users have not explored this function fully and incorporated the certification process into their monthly program management procedures.

Another reason was the time required to certify information. The detailed review and certification of reported results at the activity level is a time-consuming process; project implementers report on task-level activities each month, and the COR and AOR need to review and certify these reported results for each activity.

Not conducting regular reviews on reported results has hurt data quality and results that the mission reported on its programs. For example, six of the eight performance audit reports RIG/Cairo issued from October 2010 through September 2013 included recommendations to improve or correct problems noted with reported results of USAID/West Bank and Gaza projects.

Furthermore, inaccurate or incomplete data could affect the mission's decision-making. Not only does the mission use information from Geo-MIS to make informed decisions and assess program performance, but it also uses this data to report on the performance of its programs with an annual budget of $350 million. For example, information from Geo-MIS was used for the mission's annual performance plan and report and was cited in responding to requests from USAID officials in Washington.

To address improvement needed to the Geo-MIS certification process, we are making the following recommendations.

Recommendation 36. *We recommend that USAID/West Bank and Gaza review and document the frequency and level of certification required by the contracting officer's representatives and agreement officer's representatives in the Geo-Management Information System.*

Recommendation 37. *We recommend that USAID/West Bank and Gaza implement a policy to periodically validate contracting officer's representatives and agreement officer's representatives compliance with Geo-Management Information System certification requirements.*

EVALUATION OF MANAGEMENT COMMENTS

In its comments on the draft report, USAID/West Bank and Gaza and USAID/Office of Security agreed with all the recommendations except for Recommendation 14.

USAID/Office of Security was asked to evaluate the findings and related recommendations that dealt with the mission's PVS. In its management comments, the office stated that the Agency has been operating two PVSs: the system used by the mission and a second one operated by the Agency's Chief Information Office.

In response to the draft report, a Washington-based working group examined the capabilities and functions of these two systems and the State Department's vetting system with the intention of using one system throughout USAID. The group decided the best of the three was the one operated by the Chief Information Office. The Office of Security plans to merge the two USAID systems, initiate a new certification and accreditation for this system, and work with the Chief Information Office to develop a plan of action and milestones to correct the deficiencies this audit identified.

During the audit, the mission took corrective action on Recommendations 21, 23, 25, and 33, and we acknowledged final action was taken on those four upon issuance of the draft report.

Based on our evaluation of management comments provided by USAID/West Bank and Gaza and USAID/Office of Security, we acknowledge management decisions for Recommendations 1 through 37. Final action has been taken on Recommendations 14, 28, and 35 upon issuance of the final report. Therefore the mission has completed final action on Recommendations 14, 21, 23, 25, 28, 33, and 35.

Recommendations 1, 2, 4, 5, 8, and 9. The mission agreed with these recommendations and plans on completing corrective action by December 31, 2014. Based on the mission's comments, we acknowledge that management decisions have been reached on these recommendations.

Recommendations 10, 15, 16, 17, 20, 24, 26, 27, 29, 30, 31, 34, 36, and 37. The mission agreed with these recommendations and plans on completing corrective action by September 30, 2014. Based on the mission's comments, we acknowledge that management decisions have been reached on these recommendations.

Recommendation 11. The mission agreed with the recommendation to implement contingency plan testing procedures and anticipates completing corrective action by October 31, 2014. Based on the mission's comments, we acknowledge that a management decision has been reached.

Recommendation 14. The mission and USAID/Office of Security disagreed that an alternate processing site was necessary for the PVS portal because the mission could revert to manually processing vetting requests in case of a system failure. We acknowledge that a management decision has been made and final action has taken place.

Recommendation 18. USAID/West Bank and Gaza agreed with the recommendation to have procedures in place to perform annual reviews of PVS, PVS portal, and Geo-MIS access rights. The mission anticipates completing these procedures for PVS and the portal by April 30, 2014, and for Geo-MIS by September 30, 2014. We acknowledge that a management decision has been made.

Recommendations 21, 23, 25, and 33. The mission agreed with the recommendations, reached a management decision, and took final action on February 10, 2014.

Recommendation 22. USAID/West Bank and Gaza agreed with the recommendation to review segregation of duties for PVS, PVS portal, and Geo-MIS system administrators. The review of PVS and the portal was completed, and the mission provided supporting documentation. For Geo-MIS, the mission anticipates completing its review by September 30, 2014. We acknowledge that a management decision has been made. Although corrective action has been completed for PVS and PVS portal, the recommendation cannot be closed until final action is completed on Geo-MIS.

Recommendation 28. The mission agreed with the recommendation and provided security training to its system administrators. Based on the documentation provided, we acknowledge that a management decision has been made and final action has taken place.

Recommendation 35. The mission agreed with the recommendation and has made changes to the PVS portal. Based on management comments and supporting documentation provided, we acknowledge that a management decision has been made and that final action has taken place.

Recommendation 3, 6, 7, 12, 13, 19, and 32. The Office of Security agreed with these recommendations and plans to work with USAID/Chief Information Office to develop a plan of action and milestones to correct the deficiencies identified by this audit. The office plans to merge the mission's PVS with the Chief Information Officer's system, which should create a single certified, accredited vetting system for the Agency. The Office of Security plans to have a plan developed by December 31, 2014, and the plan will be completed by December 31, 2015. Based on USAID's action plan, we acknowledge management decisions have been reached on these recommendations.

SCOPE AND METHODOLOGY

Scope

RIG/Cairo conducted this audit 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 objective. We believe the evidence obtained provides that basis.

The purpose of this audit was to determine whether USAID/West Bank and Gaza implemented minimum-security controls to protect the confidentiality, integrity, and availability of PVS, the PVS NGO Portal, and Geo-MIS, as required by NIST.

RIG/Cairo conducted the audit at the USAID/West Bank and Gaza office from September 30 through December 19, 2013, and covered activities from system implementation through October 3, 2013. As of September 30, 2013, $1.5 million had been obligated and $1.4 million disbursed for the Geo-MIS system, and approximately $1.6 million had been obligated and disbursed for both PVS and the portal. The audit reviewed the Agency's accounting records but did not test invoices or payments made to the respective contractors.

For the Geo-MIS systems, we assessed the significant controls related to system implementation, reporting, and review of performance measures and indicators. We reviewed and assessed the internal controls in place to monitor system activity and security, including reviewing user log-on procedures, information submissions, and other procedures. Specifically we tested 22 NIST security controls identified in Appendix III.

Methodology

For all systems, we used the criteria for information security controls required for all U.S. Government information systems contained in NIST's FIPS and special publications. Selected controls evaluated are in the table in Appendix III.

For the PVS system, we reviewed Executive Order 13224, which blocks property and prohibits transactions with people who commit, threaten to commit, or support terrorism. We interviewed officials from the USAID/Office of Security to gain an understanding of the Agency's management controls over vetting. We also assessed the significant controls related to system implementation.

We used random number statistical sampling on a universe of 136 PVS and portal users and 135 Geo-MIS users for testing to project the results to the intended population. To obtain a 95 percent confidence level, at less than 5 percent error and 2.4 percent precision, the audit team interviewed 83 account users from all three systems. The team also conducted eight site visits to interview implementing partners in Israel and the West Bank using the systems.

MANAGEMENT COMMENTS

USAID | WEST BANK/GAZA
FROM THE AMERICAN PEOPLE

UNCLASSIFIED

Date: March 14, 2014

To: Regional Inspector General, Cairo, Catherine Trujillo

From: Mission Director, USAID West Bank and Gaza, R. David Harden /S/

Through: Deputy Mission Director, Jonathan Kamin /S/

Subject: Mission's Comments on the Draft Audit Report of USAID/West Bank and Gaza's Partner Vetting and Geo-Management Information Systems

Draft Audit Report No. 6-294-14-00X-P dated February 10, 2014

USAID/West Bank and Gaza (USAID/WBG) wishes to thank the Regional Inspector General/Cairo (RIG/Cairo) for conducting the combined audit of the three independent systems in this report, Mission's Partner Vetting System (PVS), the PVS Nongovernmental Organization Portal (PVS Portal) and the Geo-Management Information System (Geo-MIS). The Mission appreciates this opportunity to comment on the draft audit report and the recommendations therein as the RIG/Cairo prepares to issue the final draft report. The subject draft audit report has been thoroughly reviewed by the Office of Contracts Management (OCM) and the Program and Project Development Office (PPDO) in collaboration with other offices of the Mission.

As is noted in the draft report, the Mission has taken final corrective actions pertaining to Recommendations No. 21, 23, 25 and 33, and as such, these have been closed by RIG/Cairo upon issuance of the subject draft report.

In addition, the following recommendations will be directly and separately addressed by the USAID Office of Security in Washington D.C.: Recommendations No. 3, 6, 7, 12, 13, 19, and 32.

Therefore, following are the Mission's comments and/or corrective actions taken on Recommendations No. 1, 2, 4, 5, 8, 9, 10, 11, 14, 15, 16, 17, 18, 20, 22, 24, 26, 27, 28, 29, 30, 31, 34, 35, 36, and 37.

Recommendation No. 1:

We recommend that USAID/West Bank and Gaza implement written risk assessment procedures documenting roles and responsibilities of mission staff, and periodic review for Geo-Management Information System in accordance with National Institute for Standards and Technology Special Publication 800-53.

Response:
USAID/WBG agrees with the recommendation. PPDO in partnership with USAID/WBG Executive Office (EXO/IT) are working with the Chief Information Office in Washington (CIO) to complete all of the required templates and to develop the scope of work for a contractor (assessor). The contractor will help the Mission develop and implement written risk assessment procedures documenting roles and responsibilities of the Mission's staff and procedures for periodic reviews for Geo-Management Information System (Geo-MIS) in accordance with the National Institute for Standards and Technology Special Publication 800-53. The Mission expects to complete these actions by December 31, 2014.

Recommendation No. 2:
We recommend that USAID/West Banks and Gaza document a risk assessment of the Geo-Management Information System in accordance with federal information processing standards 199 and National Institute for Standards and Technology Special Publication 800-30, and categorize the system as low-, moderate-, or high-risk.

Response:
USAID/WBG agrees with the recommendation. PPDO in partnership with EXO/IT is working with the CIO to complete all of the required templates and to develop the scope of work for a contractor (assessor). The contractor will help the mission document a risk assessment for Geo-MIS in accordance with federal information processing standards 199 and National Institute for Standards and Technology Special Publication 800-30. The contractor will also categorize the system as low-, moderate-, or high-risk. The Mission expects to complete these actions by December 31, 2014.

Recommendation No. 4:
We recommend that USAID/West Bank and Gaza prepare a written security assessment of the Geo-Management Information System in accordance with National Institute for Standards and Technology Special Publication 800-53.

Response:
USAID/WBG agrees with the recommendation. PPDO in partnership with EXO/IT is working with the CIO to complete all of the required templates and to develop the scope of work for a contractor (assessor). The contractor will help the mission prepare a written security assessment on Geo-MIS in accordance with the National Institute for Standards and Technology Special Publication 800-53. The Mission expects to complete these actions by December 31, 2014.

Recommendation No. 5:
Based on the results of the security assessment, we recommend that USAID/West Bank and Gaza document its plan of action and milestones for the Geo-Management Information System in accordance with National Institute for Standards and Technology Special Publication 800-53.

Response:
USAID/WBG agrees with the recommendation. PPDO in partnership with EXO/IT is working with the CIO to complete all of the required templates and to develop the scope of work for a contractor (assessor). Upon the contractor's completion of the security assessment, the contractor will help the Mission document its plan of action and milestones for Geo-MIS in accordance with National Institute for Standards and Technology Special Publication 800-53. The Mission expects to complete these actions by December 31, 2014.

Recommendation No. 8:
We recommend that USAID/West Bank and Gaza obtain a certified authorization to operate the Geo-Management Information System from the Agency's Chief Information Security Officer in accordance with Automated Directives System 545.

Response:
USAID/WBG agrees with the recommendation. PPDO in partnership with EXO/IT is working with the CIO to complete all of the required templates and to develop the scope of work for a contractor (assessor). The contractor will help the mission meet all requirements to obtain authorization in accordance with ADS 545. The Mission expects to complete these actions by December 31, 2014.

Recommendation No. 9:
We recommend that USAID/West Bank and Gaza implement a security plan in accordance with National Institute for Standards and Technology Special Publications 800-53 and 800-18 for the Geo-Management Information System.

Response:
USAID/WBG agrees with the recommendation. PPDO in partnership with EXO/IT is working with the CIO to complete all of the required templates and to develop the scope of work for a contractor (assessor). The contractor will help the Mission implement a security plan in accordance with National Institute for Standards and Technology Special Publication 800-53 and 800-18 for the Geo-Management Information System. The Mission expects to complete these actions by December 31, 2014.

Recommendation No. 10:
We recommend that USAID/West Bank and Gaza implement comprehensive contingency plan procedures in accordance with National Institute for Standards and Technology Special Publications 800-53 and 800-34 for its information systems including the Geo-Management Information System.

Response:
USAID/WBG agrees with the recommendation. USAID/WBG is currently implementing comprehensive contingency plan procedures in accordance with National Institute for Standards and Technology Special Publication 800-53 and 800-34 for its General Services Network, which includes the Geo-MIS. The Mission expects to complete these actions by September 30, 2014.

Recommendation No. 11:
Upon completion of the Geo-Management Information System contingency plan, we recommend that USAID/West Bank and Gaza implement procedures to test its plan annually and update the contingency plan as needed based on the results.

Response:
USAID/WBG agrees with the recommendation. Upon completion of the contingency plan for Geo-MIS, USAID/WBG will test its plan annually (with the first test to be completed by October 31, 2014) and update the contingency plan as needed based on the results. The Mission expects to complete these actions by October 31, 2014.

Recommendation No. 14:
We recommend that USAID/West Bank and Gaza coordinate with USAID/Office of Security to identify an alternate processing site for the Partner Vetting System Nongovernmental Organization Portal and incorporate the site into its contingency plan.

Response:
The Mission and USAID/Office of Security disagree with this recommendation. The Mission does not need to identify an alternate processing site because it can revert to manual processing of vetting requests in case of a system failure. While anti-terrorism vetting is a statutorily required procedure for the Mission, the PVS Portal's function in the vetting process is not essential per NIST SP 800-53 (and in fact processing was performed manually until September 2012). Therefore manual processing would be an adequate contingency plan that would allow the Mission to meet its statutory vetting requirements.

Furthermore, per the Business Impact Assessment (BIA) of the PVS Portal, which was submitted to the RIG, the PVS Portal's purpose is "to provide functionality to NGO's to complete, submit, and track Partner Information Forms (PIFs)." Since the Mission's vetting procedures began in 2006 and until the Portal was launched in 2012, the Mission's partners and staff conducted these functions manually. In fact, even today, some of our partners do not have access to the PVS Portal due to the duration of their project or other factors, and the Mission still processes their vetting requests manually. Therefore, the Mission has decided that in case of a system disruption we would revert to manual operations until system recovery is resumed at original site.

Recommendation No. 15:
We recommend that USAID/West Bank and Gaza include recovery of the information systems once normal operations return in its Geo-Management Information System contingency plan.

Response:
USAID/WBG agrees with the recommendation. USAID/WBG will establish thorough plans, procedures, preventive measures, recovery strategies, and technical considerations appropriate to Geo-MIS in order to enable system recovery within the allowable downtime based on the business impact analysis following a service disruption. The Mission expects to complete these actions by September 30, 2014.

Recommendation No. 16:

We recommend that USAID/West Bank and Gaza modify the Geo-Management Information System to include a transaction recovery system, such as transaction rollback or transaction journaling, to assist in the recovery of the database in the event of a failure, as required by National Institute for Standards and Technology Special Publication 800-53.

Response:
USAID/WBG agrees with the recommendation. USAID/WBG will work with Systematics, the Geo-MIS contractor, to implement an appropriate transaction recovery system that will assist in the recovery of the database in the event of a failure, as required by National Institute for Standards and Technology Special Publication 800-53. The Mission expects to complete these actions by September 30, 2014.

Recommendation No. 17:
We recommend that USAID/West Bank and Gaza modify its Geo-Management Information System access control procedures and include the topics required by National Institute for Standards and Technology Special Publication 800-53.

Response:
USAID/WBG agrees with the recommendation. USAID/WBG will modify Geo-MIS access control to comply with the guidance of NIST SP 800-53. Annual reviews of the policy and its documentation will become part of the policy. The Mission expects to complete these actions by September 30, 2014.

Recommendation No. 18:
We recommend that USAID/West Bank and Gaza implement procedures (1) defining and requiring periodic review of user accounts and roles, and (2) deactivating invalid user accounts within the Geo-Management Information System, Partner Vetting System, and Partner Vetting System Nongovernmental Organization Portal as required by National Institute for Standards and Technology Special Publication 800-53.

Response:
USAID/WBG agrees with the recommendation.

For the PVS and PVS Portal, the USAID/WBG will, by April 30, 2014, have procedures in place to conduct periodic reviews of user accounts and roles and to deactivate invalid user accounts within the PVS and the PVS Portal.

For Geo-MIS, USAID/WBG will modify policies and procedures in order to require annual reviews of user accounts and roles and deactivate invalid user accounts in line with NIST SP 800-53 guidance. The Mission expects to complete these actions with regards to Geo-MIS by September 30, 2014.

Recommendation No. 20:
We recommend that USAID/West Bank and Gaza incorporate audit trails for creation of user accounts, last user log-ons, role modifications and disabling of user accounts to Geo-

Management Information System as required by National Institute for Standards and Technology Special Publication 800-53.

Response:
USAID/WBG agrees with the recommendation. USAID/WBG will work with Systematics, the Geo-MIS contractor, to modify Geo-MIS to incorporate audit trails for creation of user accounts, last user logon, role modifications and disabling of user accounts as required by National Institute for Standards and Technology Special Publication 800-53. The Mission expects to complete these actions by September 30, 2014.

Recommendation No. 22:
We recommend USAID/West Bank and Gaza (1) review and document the review results on roles assigned to Geo-Management Information System and Partner Vetting System administrators, and (2) correct any separation of duties weaknesses noted, or document reasons for not correcting noted weaknesses.

Response:
USAID/WBG agrees with the recommendation.

For Geo-MIS, USAID/WBG will review and document segregation of duties roles assigned to the Geo-MIS System administrator and will address any weaknesses that are identified. The Mission expects to complete these actions by September 30, 2014.

For PVS, the Mission has already taken corrective actions. Please see Attachments 1A&B for details.

Recommendation No. 24:
We recommend that USAID/West Bank and Gaza document the acceptable number of user log-on attempts before a Geo-Management Information System user account is locked and incorporate this control into the Geo-Management Information System application.

Response:
USAID/WBG agrees with the recommendation. USAID/WBG has set the acceptable number of log-on attempts at 4, and this will be documented in revised Geo-MIS policies and procedures. USAID/WBG will work with Systematics, the Geo-MIS contractor, to modify Geo-MIS to block users after 4 failed login attempts. Only the System Administrator will be able to unlock the system. The Mission expects to complete these actions by September 30, 2014.

Recommendation No. 26:
We recommend that USAID/West Bank and Gaza define and document its session lock criteria for the Geo-Management Information System in management-approved procedures.

Response:
USAID/WBG agrees with the recommendation. Based on the categorization of the system (low, moderate, high) USAID/WBG will modify Geo-MIS policies and procedures to define and document session lock criteria, as required according to the relevant security control baseline. If

the system is categorized as low risk, session lock access control (AC-11) is not applicable, and therefore no action is needed. The Mission expects to complete these actions by September 30, 2014.

Recommendation No. 27:
We recommend USAID/West Bank and Gaza modify the Geo-Management Information System to prevent the display of data once the system locks the session.

Response:
USAID/WBG agrees with the recommendation. Based on the categorization of the system (low, moderate, high) USAID/WBG will work with Systematics, the Geo-MIS contractor, to modify Geo-MIS to prevent the display of data once the system locks the session. However, if the system is categorized as low risk, session lock access control (AC-11) is not applicable, and therefore no action is needed. The Mission expects to complete these actions by September 30, 2014.

Recommendation No. 28:
We recommend that USAID/West Bank and Gaza provide training to the system administrators of the Partner Vetting System, Partner Vetting System Nongovernmental Organization Portal and Geo-Management Information System on information system security and security requirements for federal information systems.

Response:
USAID/WBG agrees with the recommendation. The Mission has already taken corrective action. In January 2014, the Mission's Systems Manager attended the mission accreditation training and passed the associated exam. He later conducted training on March 7th for the administrators of the Geo-MIS, PVS, and PVS Portal. Please see Attachment 2 for the training slides and sign-in sheet. Therefore, the Mission considers that final corrective action has been taken on this recommendation and kindly requests the closure of this recommendation upon issuance of the final report.

Recommendation No. 29:
We recommend that USAID/West Bank and Gaza implement a comprehensive identification and authentication policy and procedures for the Geo-Management Information System to comply with the guidance of National Institute for Standards and Technology Special Publication 800-53.

Response:
USAID/WBG agrees with the recommendation. USAID/WBG will develop and implement comprehensive identification and authentication policy and procedures for Geo-MIS to comply with NIST SP 800-53. USAID/WBG will review the policies and procedures annually and update them as needed. The Mission expects to complete these actions by September 30, 2014.

Recommendation No. 30:
Following the implementation of the identification and authentication policy and procedures for the Geo-Management Information System, we recommend that USAID/West Bank and Gaza

implement procedures to conduct periodic reviews and document the review results to comply with the guidance of National Institute for Standards and Technology Special Publication 800-53.

Response:
USAID/WBG agrees with the recommendation. USAID/WBG will document annual reviews of its policies and procedures to comply with NIST SP 800-53. The Mission will complete these actions by September 30, 2014.

Recommendation No. 31:
We recommend that USAID/West Bank and Gaza incorporate authenticator management controls in the Geo-Management Information System to enforce minimum password complexity; minimum number of changed characters when new passwords are created; encrypted representations of passwords for storage and transmission; password minimum and maximum lifetime restrictions; rules governing recycling of password; and the use of a temporary password for system log-ons with an immediate change to a permanent password, in compliance with National Institute for Standards and Technology Special Publication 800-53.

Response:
USAID/WBG agrees with the recommendation. USAID/WBG will work with Systematics, the Geo-MIS contractor, to modify Geo-MIS to incorporate authenticator management controls as required by NIST SP 800-53. The changes to be made in Geo-MIS include:

1. Require the password to be stronger in the following way: must be at least ten characters long, contain at least one upper case letter, one digit, and one special character.
2. Require users to change their password annually. This will be accomplished by setting a common date for expiration of all passwords; January 1st and July 1st.
3. Allow only the Geo-MIS administrator to assign an initial temporary password to a new user; send an email to the user with the new user-ID and temporary password; and require the user to change the temporary password to a permanent password immediately after the first successful login.
4. Ensure that passwords are encrypted during login and storage.

The Mission expects to complete these actions by September 30, 2014.

Recommendation No. 34:
We recommend that USAID/West Bank and Gaza use a secure session for transmitting data from its implementing partners.

Response:
USAID/WBG agrees with the recommendation. USAID/WBG will work with Systematics, the Geo-MIS contractor, to modify Geo-MIS to use secure sessions for transmission of data with all users. The Mission expects to complete these actions by September 30, 2014.

Recommendation No. 35:

We recommend that USAID/West Bank and Gaza in coordination with USAID/Office of Security implement necessary changes to the Partner Vetting System Nongovernmental Organization Portal to eliminate restrictions on age limits in the birth date fields in the Partner Information Form and allowing changes made to be reflected in the form.

Response:
The Mission and USAID/Office of Security agree with this recommendation and have already taken the following corrective actions:

(1) Birth Date Inputs: The PVS Portal now accepts birth dates prior to the year 1940. Please see Attachment 3A for a screen shot of the Portal accepting a birthdate of an individual who was born prior to 1940.
(2) Birth Date Inputs: The PVS Portal now accepts individuals who are younger than 18 years of age. In compliance with Mission Order 21, Anti-Terrorism Procedures, the Portal accepts individuals who are 16 years of age or older. Please see Attachment 3B for a screen shot of the Portal accepting a birthdate of an individual who is 16 years old.
(3) Changes Not Saved: The PVS Portal now retains changes made to correct erroneous information in vetting forms once the forms are saved. Please see Attachment 3C for the release notes of changes that were made to the Portal. Paragraph number six "Editing Individual and Organization" refers to the fixing of this problem.

Therefore, the Mission considers that final corrective action has been taken on this recommendation and kindly requests the closure of this recommendation upon issuance of the final report.

Recommendation No. 36:
We recommend that USAID/West Bank and Gaza review and document the frequency and level of certification required by the contracting officer's representatives and agreement officer's representatives to in the Geo-Management Information System.

Response:
USAID/WBG agrees with the recommendation. USAID/WBG will revise the C/AOR certification training materials, conduct training on an annual basis for C/AORs, develop checklists for C/AORs usage during the certification, make sure that Geo-MIS is sending monthly and quarterly reminders to the designated C/AOR and his/her alternate to complete the certification with an attached list of activities to be certified. The System Administrator will generate quarterly monitoring reports from the system detailing the frequency and level of certification by each C/AOR. The Mission expects to complete these actions by September 30, 2014.

Recommendation No. 37:
We recommend that USAID/West Bank and Gaza implement a policy to periodically validate contracting officer's representative's and agreement officer's representative's compliance with Geo-Management Information System certification requirements.

Response:

USAID/WBG agrees with the recommendation. USAID/WBG will update the Geo-MIS usage policy to include a mission plan for monitoring the C/AOR certification process on a quarterly basis to ensure compliance. The Mission expects to complete these actions by September 30, 2014.

Appendix II

April 17, 2014

MEMORANDUM

TO: SAC RIG/Cairo, Catherine Trujillo
RIG/Cairo, David Thomanek

FROM: SEC/ISP Division Chief, David Blackshaw /s/

SUBJECT: Audit of USAID/West Bank and Gaza's Partner Vetting and Geo-Management Information Systems (Report No. 6-294-14-00X-P)

SEC/ISP has reviewed the subject draft audit report and agreed with the findings.

The response to the OIG draft took longer than expected due to the Agency had two Partner Vetting Systems (PVS) systems. The PVS working group (WG) consisting of M/OAA, LPA, GC, SEC, M/CIO and M/MPBP recognized maintaining two IT systems was not cost-effective. The PVS WG took on several intra-agency discussions, including with USAID/West Bank and Gaza (WBG), to develop a corporate approach to enhance the PVS application. We examined which system would be the optimum to use -- WBG PVS system, M/CIO PVS system and State's RAM PVS system evaluating all capabilities and functionalities. The decision was M/CIO PVS system was the best system to use for the Agency.

On April 8, 2014, the PVS WG received correspondence that WBG agreed to a "one system" option. The PVS WG will ensure WBG functionality will not be lost in the merger.

Our approach to correct the outstanding recommendations 3, 6, 7, 12, 13, 14, 18, 19, 22, 28, 32 and 35 which are associated with the WBG PVS system is merge the two systems, initiate a new Certification & Accreditation (C&A) and working with M/CIO develop POA&M to correct all deficiencies. In discussion within the PVS WG, funding is available to take this approach.

The PV WG approach is currently developing a VROM LOE to develop a complete plan by December 31, 2014. Implementation of the plan will take one-year after a complete plan is completed, December 31, 2015.

Security Controls Tested and Results

		Control Met		
NIST Control	**Description**	**Geo-MIS**	**PVS**	**PVS NGO Portal**
RA-1	Risk Assessment Policy and Procedures	No	Yes	Yes
RA-2	Security Categorization	No	N/A*	Yes
RA-3	Risk Assessment	No	N/A**	Partial
CA-2	Security Assessments	No	Yes	Yes
CA-5	Plan of Action and Milestones	No	N/A***	Partial
CA-6	Security Authorization	No	N/A****	Yes
PL-2	Security Plan	No	Yes	Yes
CP-1	Contingency Plan Policies and Procedures	Partial	Yes	Yes
CP-2	Contingency Plan	Partial	N/A*****	Partial
CP-4	Contingency Plan Testing	No	Partial	Partial
CP-7	Alternate Processing Site	Yes	Yes	No
CP-10	Information System Recovery	No	Yes	Yes
AC-1	Access Control Policy and Procedures	Partial	Yes	Yes
AC-2	Account Management	Partial	Partial	Partial
AC-5	Separation of Duties	Partial	Partial	Yes
AC-6	Least Privilege	Yes	Partial	Yes
AC-7	Unsuccessful Log-on Attempts	No	Yes	Yes
AC-8	System Use Notification	Partial	Yes	Yes
AC-11	Session Lock	Partial	Yes	Yes
IA-1	Identification and Authorization Policies and Procedures	Partial	Yes	Yes
IA-5	Authenticator Management	No	Yes	Partial
SC-23	System Authenticity	No	Yes	Yes

* This control was not tested because security authorization was already tested in Washington, D.C.
** This control was not tested because risk assessment was already tested in Washington, D.C.
*** This control was not tested because the plan of action and milestones were already tested in Washington, D.C.
**** This control was not tested because security authorization was already tested in Washington, D.C.
***** This control was not tested because the contingency plan was already tested in Washington, D.C.

U.S. Agency for International Development
Office of Inspector General
1300 Pennsylvania Avenue, NW
Washington, DC 20523
Tel: 202-712-1150
Fax: 202-216-3047
http://oig.usaid.gov