PEACE CORPS

Office of INSPECTOR GENERAL

Our Mission:

Through audits, evaluations, and investigations, the Office of Inspector General provides independent oversight of agency programs andoperations in support of the goals set forth in the Peace Corps Act while making the best use of taxpayer dollars.

Summary of Internal Control Issues Over the Peace Corps' Financial Reporting

FISCAL YEAR 2017

Background

We contracted with Kearney, an independent certified public accounting firm, to audit the Peace Corps' consolidated financial statements as of September 30, 2016 and 2017. The audit was conducted in accordance with auditing standards generally accepted in the United States of America; the standards applicable to financial audits contained in Government Auditing Standards, issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) Bulletin No. 17-03, Audit Requirements for Federal Financial Statements.

As part of their review, Kearney considered the Peace Corps' internal controls over financial reporting and compliance with provisions of applicable laws, regulations, contracts, and grant agreements in order to determine their auditing procedures for the purpose of expressing an opinion on the financial statements. However, Kearney does not provide assurance on internal control over financial reporting or on compliance. Accordingly, they do not express an opinion on the effectiveness of the Peace Corps' internal control over financial reporting or on its compliance.

Results

The results of Kearney's review of internal controls identified no material weaknesses, two significant deficiencies, and one instance of reportable non-compliance. Furthermore, Kearney noted five additional concerns regarding internal controls that do not rise to the level of material weakness or significant deficiency. These concerns are reported in the following attached report.

Results

The 22 recommendations made in Kearney's reports are intended to assist in improving the Peace Corps' internal control or other operating efficiencies.

Contact

Have questions? Need to talk to us?

Hotline

Confidentially report fraud, waste, abuse, or mismanagement in the Peace Corps.

Online: www.peacecorps.gov/OIG/

Email: OIG@peacecorpsoig.gov

Phone: (202) 692-2915

Mail: Peace Corps
Office of Inspector General
P.O. Box 57129
Washington, DC 20037-7129

General Information

Talk to OIG staff about general business.

Online: www.peacecorps.gov/OIG

Twitter: @PCOIG

Phone: (202) 692-2900

KEARNEY& COMPANY

1701 Duke Street, Suite 500, Alexandria, VA 22314
PH: 703.931.5600, FX: 703.931.3655, www.kearneyco.com

MANAGEMENT LETTER

To the Chief Executive Officer and Inspector General of the Peace Corps

In planning and performing our audit of the United States Peace Corps' (Peace Corps) consolidated financial statements as of and for the year ended September 30, 2017, in accordance with auditing standards generally accepted in the United States of America; standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) Bulletin No. 17-03, *Audit Requirements for Federal Financial Statements*, Kearney & Company, P.C. (defined as "Kearney," "we," and "our" in this letter) considered the Peace Corps' internal control over financial reporting and compliance with provisions of applicable laws, regulations, contracts, and grant agreements in order to determine our auditing procedures for the purpose of expressing an opinion on the financial statements and not to provide assurance on internal control over financial reporting or on compliance. Accordingly, we do not express an opinion on the effectiveness of the Peace Corps' internal control over financial reporting or on its compliance.

Following this Management Letter, we have attached our *Independent Auditor's Report on Internal Control Over Financial Reporting and Compliance with Laws, Regulations, Contracts, and Grant Agreements*, dated November 7, 2017. In that report, we noted no material weaknesses, two significant deficiencies, and one instance of reportable non-compliance. These items are not repeated in this letter, as they are explained in detail in that attached report.

Although not considered to be material weaknesses, significant deficiencies, or material non-compliances, we noted certain matters involving internal control and other operational matters that are presented in this letter for the Peace Corps' consideration. These comments and recommendations are intended to assist in improving the Peace Corps' internal control or result in other operating efficiencies. In the five signed Notifications of Findings and Recommendations (NFR), dated November 6, 2017, the Peace Corps concurred in concept with the findings and recommendations noted herein. We have not considered the Peace Corps' internal control or compliance since November 7, 2017.

We appreciate the courteous and professional assistance that the Peace Corps' personnel extended to us during our audit. We would be pleased to discuss our comments and recommendations with the Peace Corps at any time.

KEARNEY& COMPANY

The purpose of this letter is solely to communicate other deficiencies in internal control or non-compliances noted during the audit to management and those charged with governance and not to provide an opinion on the effectiveness of the entity's internal control or on compliance. Accordingly, this communication is not suitable for any other purpose.

Alexandria, Virginia
January 4, 2018

KEARNEY& COMPANY

MANAGEMENT LETTER COMMENTS

MODIFIED REPEAT MANAGEMENT LETTER COMMENTS

1. Timely De-Obligation of Unliquidated Obligations (ULO)

Unliquidated Obligations (ULO) represent binding agreements for goods and services that have not yet been delivered or received and will require future outlays. Agencies should maintain policies, procedures, and information systems to ensure that ULOs represent current required Federal outlays. Failure to maintain an effective ULO control environment may result in difficulties in managing funds, improper payments, inaccurate budgetary reports, and violations of Federal regulations.

Finding:

The Peace Corps reported domestic and overseas ULOs worth $90 million as of June 30, 2017. Kearney & Company, P.C. (Kearney) evaluated the validity and liquidation status of domestic and overseas non-Federal ULOs with a statistical sample and judgmentally sampled the 10 largest domestic Federal ULOs. The combined 45 domestic and overseas ULOs sampled had a recorded value of $1.4 million.

- Sixteen of the 35 statistically sampled non-Federal ULOs valued at $350,920 should have been de-obligated. The identified exceptions produced a projected likely error of approximately $565,767
- One out of 10 judgmentally sampled Federal ULOs valued at $17,500 should have been de-obligated as of June 30, 2016. This error composed 2% of the recorded Federal ULO balance.

In total, Kearney identified 17 exceptions with a recorded value of $368,420 that no longer represented future Peace Corps funding needs and should have been de-obligated during the tri-annual open obligations review.

Recommendations: Kearney recommends that the Peace Corps take steps to strengthen and better integrate the obligation process, including the following:

1. Continue to perform the tri-annual open obligations review and ensure that the ultimate disposition of open obligations is formally documented, reviewed, and certified by a senior official(s) in a timely and routine manner.
2. In addition to the scheduled tri-annual open obligation review, Headquarters (HQ) and posts should routinely review open obligations and de-obligate those that are no longer valid.
3. Following the tri-annual open obligation review, HQ and posts need to apply greater resources to close identified open obligations in a timely fashion.
4. Provide annual training on related policies and procedures to ensure consistency among posts.

2. Information Technology

Inadequate Account Management and Password Parameters

Background:

Computer resource owners should identify the specific user, or class of users, authorized to obtain direct access to each resource for which they are responsible. They should disable and remove unnecessary accounts (i.e., inactive, generic, and test accounts) in a timely manner. Failure to disable unnecessary accounts could result in security breaches, corruption of data integrity, or impaired availability of data to support financial reporting and operations.

Password policies are necessary to protect the confidentiality of information and the integrity of systems by keeping unauthorized users out of computer systems. Password policies of agencies may vary in their complexity depending on the perceived need to secure the organization's assets. Passwords that are too short increase the speed and ease of cracking passwords by brute force, dictionary, or other password attacks.

Account Management Findings:

Kearney reviewed the Peace Corps' user listing and user management policies and procedures. We noted that the Peace Corps has not implemented effective account management policies and procedures to ensure that only current users are configured in the systems. The Peace Corps' user listing contains user accounts that exceed normal expectations based on the Peace Corps' organization chart, system users, and complexity of the system. Our analysis identified the following control gap weaknesses, which resulted in the excessive number of users.

The Peace Corps' account management policy and procedures do not adequately define or implement a process to ensure inactive accounts are disabled in a timely manner. The Peace Corps' management have not implemented an effective account management policy, as required, for staff, volunteer, generic, service, and test accounts. While the policies are comprehensive, the Peace Corps has not conducted an effective clean-up of user accounts. We noted that approximately 40% of all Peace Corps user accounts were not managed as required by policy. We also identified user account types which are shared or not associated with a specific user. (***Repeat and Modified Condition***)

Password Parameter Findings

Kearney reviewed the Peace Corps' *System Access and Account Management Standard Operating and Procedures Guide*. We noted that the Peace Corps' policies do not require more stringent requirements for high-risk user profiles. We also noted certain account types that are not configured with a password expiration period as required by policy. (***Repeat Condition***)

Kearney also reviewed the Peace Corps' relevant *System Security Plan* (SSP). In it, the Peace Corps did not define more stringent account password requirements for higher risk, including

minimum password complexity, enforcement of character change when new passwords are created, password minimum and maximum lifetime, or password reuse. (***New Condition***)

Additionally, the Peace Corps has not configured relevant information systems to support the different password configuration and expiration requirements for higher risk accounts. The Peace Corps has also not fully developed an automatic monitoring system to replace manual monitoring. (***New Condition***)

Recommendations:

Kearney recommends that the Peace Corps consider the following corrective actions to strengthen existing access and password controls.

Condition #1: Account Management Findings

5. Develop policies and implement an automated solution to enforce automatic removal of terminated and separated personnel for all account types.
6. Develop and implement policies to perform periodic account cleanup of unused and unnecessary accounts in a timely manner.
7. Conduct an annual review and update account management policies and procedures to ensure account requirements are current, as well as balance the business with security requirements.

Condition #2: Passwords Parameter Findings

8. Update password policies to require more stringent password parameters for higher risk users addressing password character change, password length, complexity, minimum and maximum life, reuse, and protection of default vendor accounts.
9. Develop and modify system configuration settings to enforce new password requirements for privileged user accounts separate from other user accounts.
10. Ensure personnel responsible for configuring system parameters understand the financial system database password requirements.

KEARNEY& COMPANY

NEW MANAGEMENT LETTER COMMENTS

1. Information Technology

Change Management Separation of Duty Conflict

Background:

Traditional systems of internal control rely on assigning certain responsibilities to different individuals in order to separate incompatible functions. For computer processing, agencies should ensure that computer access is consistent with roles and responsibilities. Change management procedures should occur in a test environment separate from the production environment and a separate review and approval of changes before they are placed in production. Untested and unapproved changes could result in processing errors and erroneous disbursements, as well as negatively impact system performance.

Finding:

Kearney reviewed the relevant Peace Corps' SSP for financial systems and privileged user access for configuration management. The Peace Corps has not documented and implemented appropriate segregation of duties (SoD) controls in its financial information system. Specifically, the Peace Corps has not documented privileged roles or role combinations that result in a conflict of interest. Role conflicts for developers, administrators, change management, and code migrators are not documented in a SoD matrix.

We identified two instances in which the Peace Corps provisioned two privileged users to develop and promote code from the test to the production environment. In one of those instances, the access was granted by using a retired user's profile. We also identified two other instances in which users were also provisioned to promote code from the test to production environment.

In all four cases, Peace Corp did not have a business justification for providing this access. Additionally, this configuration did not provide for an independent review of test environment changes before it was placed in the production environment.

Recommendations:

Kearney recommends that the Peace Corps take the following corrective actions to address these issues:

11. Develop a SoD matrix and identify incompatible functions.
12. Implement a risk acceptance process to formally document and approve exceptions to SoD requirements that identify compensating controls, as well as how the risk is lowered or mitigated. Monitor compensating controls to verify they are in place and operating effectively.

2. Information Technology

Lack of a Process to Review National Finance Center (NFC) Service Organization Controls (SOC) Report

Background:

Agencies outsource transaction processing activities to service organizations to achieve efficiencies and subject matter expertise. While outsourced to service organizations, agencies are ultimately responsible for the accuracy of information provided by service organizations included in their financial statements. Service Organization Controls (SOC) are designed to help service organizations that provide services to other entities, building trust and confidence in the services performed and controls related to the services through the issuance of a report by an independent Certified Public Accounting (CPA) firm. The SOC 1 is a report on controls at a service organization relevant to user entities' internal control over financial reporting.

The Peace Corps utilizes the United States Department of Agriculture's (USDA) National Finance Center's (NFC) WebTA application to process time and attendance (T&A). NFC hosts a number of systems that are financially relevant to Federal agencies. NFC contracted with an Independent Public Accounting (IPA) firm to issue their SOC 1 report, which is called *SSAE No.18 Report on Controls at the NFC,* and prepared under American Institute of Certified Public Accountants' (AICPA) Statement on Standards for Attestation Engagements (SSAE) No. 18 to provide assurance that the information provided by the service provider is complete and accurate, as well as to identify risks to NFC customers. Failure to evaluate SOC reports may lead to unidentified internal control gaps, erroneous financial statements, and fraudulent transactions.

Finding:

The Peace Corps has not formally documented and implemented a procedure to annually review the *SSAE No.18 Report on Controls at the NFC.* Specifically, the Peace Corps has not assigned responsibility to stakeholders within the Human Resources (HR) Department, Office of the Chief Financial Officer (OCFO), and Office of the Chief Information Officer (OCIO) to implement the process and take corrective actions when weaknesses are identified in the SSAE No. 18 report.

Recommendations:

Kearney recommends that the Peace Corps establish an operating procedure for reviewing the SSAE No.18 report for the WebTA application. At a minimum, the Peace Corps should:

13. Create a comprehensive policy to identify all service organizations, obtain SOC 1 reports, and review SOC 1 reports for weaknesses and key control gaps.
14. Coordinate with NFC to add any key controls determined by management that are not currently in the scope of the SSAE No.18 examination.

KEARNEY& COMPANY

1701 Duke Street, Suite 500, Alexandria, VA 22314
PH: 703.931.5600, FX: 703.931.3655, www.kearneyco.com

INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND COMPLIANCE WITH LAWS, REGULATIONS, CONTRACTS, AND GRANT AGREEMENTS

To the Acting Director and Inspector General of the United States Peace Corps

We have audited the consolidated financial statements of the United States Peace Corps (Peace Corps) as of and for the year ended September 30, 2017, and we have issued our report thereon dated November 7, 2017. We conducted our audit in accordance with auditing standards generally accepted in the United States of America; the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) Bulletin No. 17-03, *Audit Requirements for Federal Financial Statements*.

Internal Control over Financial Reporting

In planning and performing our audit of the consolidated financial statements, we considered the Peace Corps' internal control over financial reporting (internal control) to determine the audit procedures that are appropriate in the circumstances for the purpose of expressing an opinion on the consolidated financial statements, but not for the purpose of expressing an opinion on the effectiveness of the Peace Corps' internal control. Accordingly, we do not express an opinion on the effectiveness of the Peace Corps' internal control. We limited our internal control testing to those controls necessary to achieve the objectives described in OMB Bulletin No. 17-03. We did not test all internal controls relevant to operating objectives as broadly defined by the Federal Managers' Financial Integrity Act of 1982 (FMFIA), such as those controls relevant to ensuring efficient operations.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect and correct misstatements on a timely basis. A material weakness is a deficiency, or combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's consolidated financial statements will not be prevented or detected and corrected on a timely basis. A significant deficiency is a deficiency, or combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Our consideration of internal control was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies; therefore, material weaknesses or significant deficiencies may exist that were not identified. Given these limitations, during our audit, we did not identify any deficiencies in internal control that we consider to be material weaknesses. However, material weaknesses may exist that have not been identified. We identified certain

deficiencies in internal control, described in the accompanying Schedule of Findings, that we consider to be significant deficiencies.

We noted certain additional matters involving internal control over financial reporting that we will report to the Peace Corps' management in a separate letter.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the Peace Corps' consolidated financial statements are free from material misstatement, we performed tests of its compliance with provisions of applicable laws, regulations, contracts, and grant agreements, with which noncompliance could have a direct and material effect on the determination of consolidated financial statement amounts. We limited our tests of compliance to these provisions and did not test compliance with all laws, regulations, contracts, and grant agreements applicable to the Peace Corps. Providing an opinion on compliance with those provisions was not an objective of our audit; accordingly, we do not express such an opinion. The results of our tests disclosed instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards* and are described in the accompanying Schedule of Findings.

The Peace Corps' Response to Findings

The Peace Corps' response to the findings identified in our audit is presented in the Agency Financial Report's "Financial Section" in the *Agency's Comments to the Independent Auditor's Report*. The Peace Corps' reviewed our report, concurs with the findings in the report, and established corrective actions for execution in fiscal year (FY) 2018. The Peace Corps' response was not subjected to the auditing procedures applied in our audit of the consolidated financial statements; accordingly, we do not express an opinion on it.

Purpose of this Report

The purpose of this report is solely to describe the scope of our testing of internal control and compliance, as well as the results of that testing, and not to provide an opinion on the effectiveness of the Peace Corps' internal control or on compliance and other matters. This report is an integral part of an audit performed in accordance with *Government Auditing Standards* and OMB Bulletin No. 17-03 in considering the entity's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

Alexandria, Virginia
November 7, 2017

KEARNEY& COMPANY

Schedule of Findings

Significant Deficiencies

I. Information Technology Security (Repeat Condition)

The United States Peace Corps' (Peace Corps) information technology (IT) internal control structure did not include a comprehensive risk analysis, proof of effective monitoring of design and performance, or evidence of the ability to identify and respond to changing risk profiles. The Peace Corps' IT control environment included design and operation weaknesses that, when combined, are considered to be a significant deficiency, as summarized below:

- During FY 2017, the Office of the Chief Information Officer (OCIO) continued the process of implementing a Continuous Monitoring Program. However, the OCIO was not able to fully implement it at the information system level in accordance with the current Information Security Continuous Monitoring (ISCM) strategy. The Federal Information Security Modernization Act of 2014 (FISMA) Evaluation Team identified the following control deficiencies:
  - The Peace Corps does not have a defined ISCM strategy
  - The Peace Corps has not developed ISCM policies and procedures to support the ISCM strategy
  - The Peace Corps has not defined roles and responsibilities of ISCM stakeholders
  - The Peace Corps has not defined metrics specifically to measure the effectiveness of its ISCM Program
- The Peace Corps does not have a robust agency-wide Risk Management Program to manage information security risks. While the OCIO formalized an overall risk management strategy in February 2014, the FISMA Evaluation Team found no evidence demonstrating that the agency was able to identify, assess, respond to, and monitor information security risk at the enterprise or business process levels. Furthermore, the Peace Corps' risk management strategy did not define the agency's information security risk profile, risk appetite, risk tolerance, and the process for communicating risks to all necessary internal and external stakeholders. Although the Senior Assessment Team (SAT) held meetings with the Chief Information Officer (CIO) and Risk Executive, these meetings were neither formalized nor consistently performed during the review period. Specifically, the FISMA Evaluation Team identified the following control deficiencies:
  - The Peace Corps did not fully maintain current authorization and assessment packages for two of the information systems tested
  - The Peace Corps has not identified and defined its requirements for an automated solution to provide a centralized, enterprise-wide (portfolio) view of risks across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards
  - The Peace Corps did not define an information security architecture that is integrated with the risk management strategy

- The Peace Corps did not maintain a formal process to perform e-authentication risk assessments according to the guidelines in Office of Management and Budget (OMB) Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*.

As defined in Generally Accepted Government Auditing Standards (GAGAS), information system controls consist of those internal controls that are dependent on information systems processing and include general and application controls. General and application controls, while effective, may not be sufficient to address and minimize the risks due to weaknesses in the Peace Corps' Information Security Program. Information Security Program policies and procedures apply to most, if not all, of the Peace Corps' information systems. The effectiveness of these procedures is a significant factor in determining the confidentiality, integrity, and availability of the information contained in the applications.

The lack of a comprehensive Continuous Monitoring Program prevents the Peace Corps from clearly understanding the security state of all of its systems over time. This also prevents the agency from effectively monitoring a dynamic IT environment with changing threats, vulnerabilities, technologies, business processes/functions, and critical missions. Without a fully implemented Continuous Monitoring Program, agency systems could incur potential damage, including system downtime, unauthorized access, changes to data, data loss, or operational failure.

Without effectively implementing a comprehensive risk management process at the agency level, the Peace Corps may be unable to address the root causes associated with existing information security risks. In addition, appropriate resources may not be effectively assigned to make the correct risk decisions to ensure the results align with the agency's business priorities.

Recommendations: Kearney & Company, P.C. (Kearney) recommends that:

1. The OCIO develop and fully implement an ISCM strategy that includes policies and procedures, defined roles and responsibilities, and security metrics to measure effectiveness.
2. The Peace Corps Director and Agency Risk Executive, in coordination with Peace Corps senior leadership, identify the agency's information security risk profile and define the agency's risk appetite and risk tolerance.
3. The Agency Risk Executive, in coordination with Peace Corps senior leadership, develop and implement an enterprise-wide risk management strategy to address how to identify, assess, respond to, and monitor security-related risks in a holistic approach across the organization, business process, and information system levels.
4. The OCIO perform all components of the Security Assessment and Authorization (SA&A) on all FISMA-reportable systems in accordance with the risk management strategy.
5. The OCIO develop an information security architecture that is integrated with the risk management strategy.

6. The OCIO develop and implement procedures for performing e-authentication risk assessments on systems according to the guidelines in OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*.

KEARNEY& COMPANY

II. Improper and Untimely Processing of Personnel Actions (Repeat Condition)

The Peace Corps processes personnel actions when an employee is hired or an existing employee experiences a change in personnel status, such as resignation, retirement, or promotion. These personnel actions are documented either on the Standard Form (SF)-50, *Notification of Personnel Action*, or the Joint Form (JF)-62A, *Personal Services Contracting Action*. Failure to process these without approved supporting documentation timely and accurately can result in erroneous compensation payments and violations of labor hours.

The Office of Personnel Management's (OPM) authority to prescribe reporting requirements covering personnel actions can be found in Section 2951, Title 5, United States Code (U.S.C.), *Reports to the OPM*. In addition, Executive Order (EO) 12107, *Relating to the Civil Service Commission and labor-management in the Federal Service*, delegates the authority to OPM to prescribe regulations relating to the establishment, maintenance, and transfer of official personnel folders.

For each processed personnel action, there will be an SF-52, *Request for Personnel Action*, or a similar agency form approved by OPM as an exception to the SF-52. The SF-52 is usually initiated by the office or supervisor who wants to create a personnel action, such as the appointment of an employee; occasionally, the Human Resource (HR) Management, Office of Management initiates the form. The requesting office completes one part of SF-52 and forwards it to others (e.g., the Budget Office) whose approval is required by the agency. The form is then sent to the Personnel Office for review and clearance by classification, staffing, and other personnel specialists, as well as for signature by the individual(s) to whom authority to approve personnel actions (appointing authority) has been delegated.

Kearney selected a sample of 23 new hire personnel actions out of a population of 160 and noted the following untimely or improperly approved actions:

- Based on our review of the SF-50, 14 employees were entered into the HR Entry, Processing, Inquiry, and Correction (EPIC) system and approved by the Director of HR after their effective date of employment. These delays ranged from one to 11 days. Details of the testing are summarized in the ***Table 1*** below. For these 14 new hire employees, we requested SF-52s and noted the following:
  - Two of the 14 SF-52s requested were not provided by HR
  - One out of 12 SF-52 Part C-1 was missing the required Budget Office approval
  - Ten out of 12 SF-52s Part C-2 were not approved by the appointed officer
  - Two of the 12 SF-52s Part C-2 were approved after the effective date by the appointed officer.

Table 1: New Hire Personnel Actions Testing Details

Sample	Effective Date of Employment	SF-52	SF-50
		Supervisor Approval Date	Director of HR Approval Date
Employee #2	January 8, 2017	September 19, 2016	January 12, 2017
Employee #3	October 16, 2016	Not provided	October 20, 2016
Employee #5	January 08, 2017	July 15, 2016	January 17, 2016
Employee #6	January 17, 2017	Not provided	January 18, 2017
Employee #7	January 08, 2017	December 14, 2016	January 18, 2017
Employee #8	December 11, 2016	October 14, 2016	December 20, 2016
Employee #9	April 16, 2017	March 1, 2017	April 21, 2017
Employee #11	October 30, 2016	October 14, 2016	November 02, 2016
Employee #14	January 15, 2017	February 11, 2016	January 17, 2017
Employee #18	December 13, 2016	October 20, 2016	December 22, 2016
Employee #19	October 30, 2016	October 7, 2016	November 7, 2016
Employee #20	October 16, 2016	April 5, 2016	October 25, 2016
Employee #22	October 2, 2016	August 5, 2016	October 13, 2016
Employee #23	January 22, 2017	December 21, 2016	January 25, 2017

Of the 14 untimely approvals by the Director of HR, 11 employees were compensated for working prior to the HR Director approval. These delays ranged from three to nine days. Details of the testing are summarized in ***Table 2*** below.

Table 2: Untimely Approval Testing Details

Sample	Effective Date of Employment	SF-52	SF-50	Pay Period Paid	Pay Period Approved	Number of Days Paid w/o Approval
		Supervisor Approval Date	Director of HR Approval Date			
Employee #2	January 8, 2017	September 19, 2016	January 12, 2017	01	01	03
Employee #3	October 16, 2016	Not provided	October 20, 2016	21	21	03
Employee #5	January 08, 2017	July 15, 2016	January 17, 2016	01	01	07
Employee #7	January 8, 2017	December 14, 2016	January 18, 2017	01	01	08
Employee #9	April 16, 2017	March 1, 2017	April 21, 2017	08	08	05
Employee #11	October 30, 2016	October 14, 2016	November 02, 2016	25	25	06
Employee #18	December 13, 2016	October 14, 2016	December 20, 2016	25	25	06
Employee #19	October 30, 2016	October 7, 2016	November 7, 2016	22	22	06

Sample	Effective Date of Employment	SF-52	SF-50	Pay Period Paid	Pay Period Approved	Number of Days Paid w/o Approval
		Supervisor Approval Date	Director of HR Approval Date			
Employee #20	October 16, 2016	April 5, 2016	October 25, 2016	21	21	08
Employee #22	October 2, 2016	August 5, 2016	October 13, 2016	20	20	09
Employee #23	January 22, 2017	December 21, 2016	January 25, 2017	02	02	03

Additionally, Kearney selected a sample of 24 separated personnel actions out of a population of 184. Specifically, we noted the following untimely or improperly approved actions:

- Based on our review of the SF-50s, 13 employees were entered into the EPIC system and approved by the Director of HR after their effective date of separation. Details of the testing are summarized in ***Table 3*** below. For these 13 separated employees, we requested their SF-52s and noted the following:
  - One of the 13 SF-52s requested was not provided by HR
  - Twelve out of 12 SF-52s Part C-2 did not have the current approving official's signature
  - Two out of 12 SF-52s Part C-1 did not have the Budget Office approval
  - Nine out of 12 SF-52s were not approved by the Director of HR until after their effective date of separation.

Table 3: Separated Personnel Actions Testing Details

Sample	Effective Date of Separation	SF-52	SF-50
		Supervisor Approval Date	Director of HR Approval Date
Employee #2	April 7, 2017	March 23, 2017	Not provided
Employee #4	December 10, 2016	December 6, 2016	Not provided
Employee #5	October 15, 2016	October 3, 2016	December 5, 2016
Employee #7	February 18, 2017	February 1, 2017	Not provided
Employee #9	May 13, 2017	April 17, 2017	May 18, 2017
Employee #10	October 29, 2016	October 3, 2016	November 1, 2016
Employee #11	January 7, 2017	January 4, 2017	January 23, 2017
Employee #12	October 21, 2016	October 28, 2016	November 2, 2016
Employee #13	May 13, 2017	April 27, 2017	June 2, 2017
Employee #15	October 15, 2016	October 11, 2016	November 2, 2016
Employee #19	December 24, 2016	December 12, 2016	Not provided
Employee #21	October 29, 2016	October 27, 2016	November 8, 2016
Employee #22	January 14, 2017	Not provided	January 26, 2017

Recommendations: Kearney recommends that the Peace Corps:

7. Develop monitoring procedures that will ensure accurate processing of personnel actions, including periodic reviews of documentation.
8. Provide training to HR staff on policies and procedures related to the entry of employees into EPIC.

* * * * *

Noncompliance and Other Matters

III. FISMA (Repeat Condition)

FISMA requires agencies to provide information security controls commensurate with the risk and potential harm of not having those controls in place. The heads of agencies and Offices of Inspectors General (OIG) are required to annually report on the effectiveness of the agencies' security programs.

As noted in its Assurance Statement, the Peace Corps disclosed an instance of noncompliance with FISMA that is required to be reported under *Government Auditing Standards* and OMB Bulletin No. 17-03, *Audit Requirements for Federal Financial Statements*.

By not complying with FISMA, the Peace Corps has potentially weakened security controls, which could adversely affect the confidentiality, integrity, and availability of information and information systems.

KEARNEY& COMPANY

APPENDIX A: STATUS OF PRIOR YEAR DEFICIENCIES

Three issues were noted relating to internal control over financial reporting in the *Independent Auditor's Report on Internal Control over Financial Reporting and Compliance with Applicable Provisions of Laws, Regulations, Contracts, and Grant Agreements* on the Peace Corps' FY 2016 consolidated financial statements.[1] ***Table 4*** presents a summary of the current-year status of these issues.

Table 4: Prior-Year Deficiencies

Deficiency	2017 Status	2016 Status
IT Internal Control Environment	Significant Deficiency	Significant Deficiency
Improper and Untimely Processing of Personnel Actions	Significant Deficiency	Significant Deficiency
Property, Plant, and Equipment (PP&E)	Closed	Significant Deficiency

[1] *Independent Auditor's Report on the Peace Corps' 2016 and 2015 Financial Statements*