



# Office of Inspector General

Office  
202.692.2900  
[peacecorps.gov/OIG](http://peacecorps.gov/OIG)  
[OIG Reports](#)

Hotline  
202.692.2915 | 800.233.5874  
[Online Contact Form](#)  
[OIG@peacecorps.gov](mailto:OIG@peacecorps.gov)

---

**To:** Carrie Hessler-Radelet, Director  
Daljit Bains, Chief Compliance Officer

**From:** Kathy A. Buller, Inspector General *Kathy A. Buller*

**Subject:** Management Advisory Report: The Peace Corps' Cloud Computing Pilot Program (IG-15-01-SR)

**Date:** March 17, 2015

The purpose of this report is to bring to your attention our concerns over the implementation of the agency's cloud computing pilot program. While we support the Peace Corps' efforts to modernize its information technology infrastructure, such as by implementing a cloud infrastructure for email and document management, we are concerned that the agency's actions during the pilot program have been inconsistent with federal mandates and acquisitions standards. We also find that the controls over information and information security during the pilot program have been lacking.<sup>1</sup>

This report makes six recommendations to improve the agency's actions regarding the cloud pilot program. We are requesting your response by **May 1, 2015**. Please provide us with an electronic copy of your signed cover memo and your response. Your response should provide your concurrence or non-concurrence with each recommendation. In addition, please use [TeamCentral](#) to document corrective action and upload documentation supporting any actions planned or implemented to address the recommendations.

Since July 2014, we have repeatedly communicated concerns about the pilot program to senior staff leading the project. However, after reviewing the agency's December 2014 Memorandum of Understanding (MOU) with the General Services Administration (GSA) and learning of the agency's plan to choose a cloud provider in the very near term, we wanted to formally outline our concerns and make recommendations aimed at improving the effectiveness and efficiency of the program while promoting compliance with federal mandates.

The cloud implementation team<sup>2</sup> has expressed the need to move forward quickly because the Peace Corps email system is not functioning at an optimal level and has experienced many unexpected outages.<sup>3</sup> Given the lack of progress over a number of years in addressing such

---

<sup>1</sup> In September 2014, the Council of Inspectors General on Integrity and Efficiency issued [a report](#) on cloud computing and found similar issues across the federal government. This report reviewed a sample of 77 commercial cloud contracts throughout the federal sector and found issues regarding compliance with federal guidance and internal agency policies.

<sup>2</sup> The cloud implementation team is the chief information officer (CIO), the director of digital integration, and the director of innovation.

<sup>3</sup> The agency, however, reports that from June to December 2014 the email server functionality was over 99 percent, with approximately 0.1 percent of downtime.

problems, the urgency in implementing a cloud solution seems misplaced.<sup>4</sup> While improving the Peace Corps systems should be a priority, the initiative should only move forward with appropriate attention placed on conducting an assessment of all solutions, consideration of data security and information integrity issues, and without unnecessary risks to the functionality of the agency-wide cloud solution.

From the start of the initiative the decision to use the GSA shared service model has appeared to be a foregone conclusion. Many staff members have expressed concerns over Google Apps' functionality and ability to meet federal requirements, but they have not shared those concerns with management since it appears that a decision to use Google Apps has already been made.

## **Background**

- May 8, 2014: Director Hessler-Radele hosts an agency all-hands meeting and asks the cloud implementation team to map out a plan for the Peace Corps to pursue a cloud computing solution that will move email and document collaboration functions to the cloud rather than managing these functions in-house.<sup>5</sup>
- July 11, 2014: The cloud implementation team announces in a memo to the Director their plan to partner with GSA to use shared services model for the cloud pilot because "it was the most efficient and least expensive method."
- July 19, 2014: The Director approves moving forward with the pilot program.
- July 22, 2014: The implementation team communicates to senior staff the decision to move forward with GSA shared services as the most efficient and cost effective approach to implement cloud-based email and collaboration.<sup>6</sup>
- August 14, 2014: The Office of the Chief Information Officer (OCIO) sends an agency-wide email announcing that GSA is the team partner for the new agency-wide collaboration and email solution and that a pilot program consisting of Google Apps would begin in September.
- September 3, 2014: Google pilot launched; Peace Corps data sent to the cloud. Pilot included approximately 260 users from headquarters offices, regional recruiting offices across the U.S., and several overseas Peace Corps posts. A group of Volunteers in participating posts is also provided access (see Table 1 for a breakdown of the Google pilot users by office).<sup>7</sup>

---

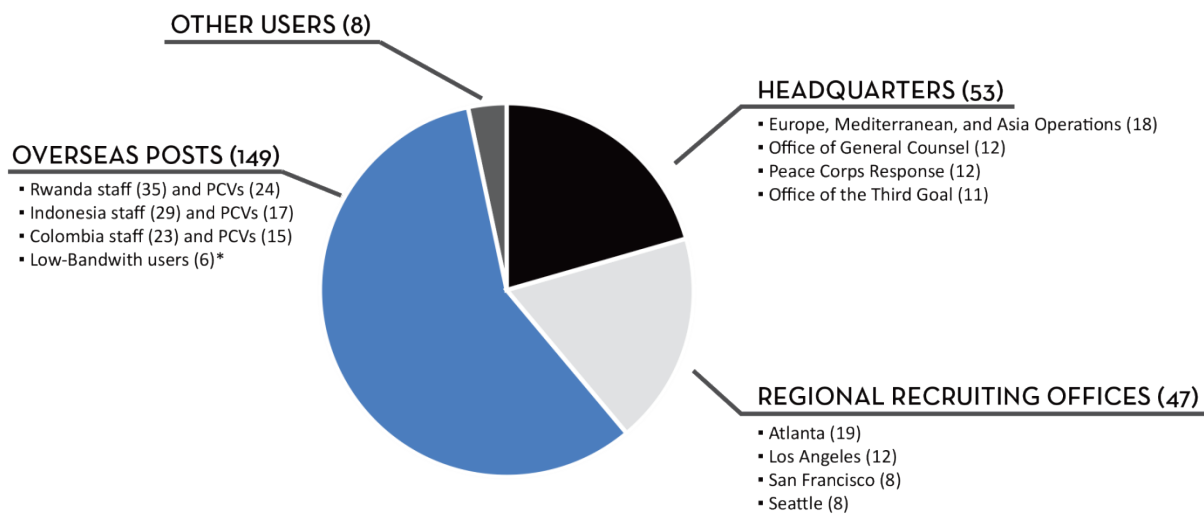
<sup>4</sup> Since fiscal year 2004, we have reported information technology as our most serious management and performance challenge facing the Peace Corps as part of the agency's Performance and Accountability Report.

<sup>5</sup> In July 2014, a senior advisor to the CIO was appointed to be the Office of the Chief Information Officer (OCIO) representative involved with cloud pilot program. For the purposes of this report, this individual is considered a member of the cloud implementation team.

<sup>6</sup> Following the announcement, OIG raised a number of concerns to the cloud implementation team regarding the pilot project including the need for data security, access to agency records, and lack of an MOU with GSA.

<sup>7</sup> The cloud implementation team and other technical staff in OCIO also had accounts, but these were not counted as part of the testing pool.

**Table 1. Breakdown of Google Pilot Users**



TOTAL USERS AS OF DEC 15, 2014= 257

\* Swaziland, Burkina Faso, The Gambia

- September 19, 2014: Analysis of alternatives document signed by the director of digital integration.
- September 29, 2014: Risk acceptance waiver signed by the agency's risk executive and the CIO (see Appendix 1).<sup>8</sup>
- December 4, 2014: The CIO and the director of digital integration sign an MOU with GSA (see Appendix 2) outlining the plan for GSA to provide cloud email service for the pilot program. It covers the pilot's scope of work, deliverables, performance schedule, and funding responsibilities.

### **Agency Rushed into Pilot Program without Considering Alternatives**

After the May 2014 all-hands announcement, the cloud implementation team made a quick decision to pursue one type of acquisition approach (no cost, shared services government provider) with one specific technology solution (Google Apps).<sup>9</sup> The analysis of alternatives document, executed in September, outlines how the cloud pilot was primarily an evaluation of the value provided by a shared services partnership with GSA. It also explains the benefits of shared services and collaborating with GSA. The analysis fails to address whether Google Apps is the best cloud platform for the Peace Corps. The analysis does not discuss why Google Apps

<sup>8</sup> A new CIO was appointed in March 2015.

<sup>9</sup> The term "shared service provider" has not been accurately presented by the cloud implementation team. A "shared service" is a very specific offering which requires OMB approval. At present, GSA's website identifies only two official shared services covering human resources, such as for personnel action processing and retirement services, and financial management services and systems. Furthermore, the solution in fact was not a "no cost" solution. In February 2015, GSA notified the Peace Corps that it would be retroactively charging the Peace Corps for services it performed during the pilot.

was chosen over the cloud service solutions, beyond it being the platform that GSA could provide through the shared services agreement.

Before the Peace Corps pursued and entered into a shared services model, a technology platform should have been researched and identified by OCIO. To effectively do this, there should have been a broad analysis of the different types of cloud platforms (e.g., Microsoft, Google) and an analysis to determine if these different platforms would meet the needs of the Peace Corps. The analysis should have included multiple offices and the identification of federal requirements and agency-specific needs. Once a technology solution was determined, the acquisition approach should have been identified (e.g., government shared services, open contract bid).

While the shared service model is beneficial to the government and part of the President's [25 Point Implementation Plan to Reform Federal Information Technology Management](#), it is important for the agency to evaluate if this shared model will return the expected benefits. The analysis of alternatives document states that the Peace Corps will be able to leverage GSA's experience and provide technical support; however, through our conversations with the cloud implementation team and OCIO staff, it is clear that they have not utilized these benefits. For example, the Peace Corps' plans to implement two-factor authentication and mobile device management are substantially different from GSA's implemented solutions.<sup>10</sup> Thus, the Peace Corps will need to rely on its internal resources and expertise for implementation of these different systems. These differing solutions will create a barrier to the Peace Corps' ability to ensure the specific platform is fully and adequately supported by the shared service provider.

Furthermore, to support this new cloud environment, the agency will need to upgrade some of its existing infrastructure and develop additional tools. For example, the agency's current remote access solution will need to be upgraded to interact properly with the Google cloud platform. This additional cost, and other similar upgrades, must be factored into a cost/benefit comparison of using a shared service provider.

### **Proper Processes Not Followed**

In implementing the cloud computing pilot program, the Peace Corps has not followed policies and procedures regarding authorities and how new systems should be identified and developed. The Peace Corps Manual section (MS) 544, "Information Technology Management," states that the CIO is responsible for developing and implementing information technology solutions, as well as for ensuring that these systems align with the Director's priorities. However, despite being a member of the cloud implementation team, the former CIO stated that she was not involved in the decision to pursue the Google Apps solution with GSA. Furthermore, the former CIO stated that OCIO was not involved in the initial planning with GSA and only became involved once help was needed to make a technical solution work.

---

<sup>10</sup> Two-factor authentication is a security mechanism that requires two types of credentials for signing onto a system and is designed to provide an additional layer of validation, by requiring two separate validation mechanisms. Typically, one is a physical validation token, and one is a logical code or password (i.e., "something they have" AND "something they know"). Both must be validated before accessing a secured service or product. A common example is the security procedure for an ATM machine which requires that a user possess a valid ATM card and PIN.

MS 114, “Delegation of Authority,” sets out the Peace Corps’ policies and procedures regarding delegations of authority. Attachment B, delegates authority to the Chief Acquisition Officer the authority to “...authorize, execute, amend, terminate, or administer all contracts, leases, agreements...” Section B of the policy further delegates all interagency agreements to the chief acquisition officer. However, the MOU with GSA was signed only by the former CIO and the director of digital integration.

While the MOU states that all costs during the pilot phase will be borne by GSA, GSA has recently communicated to the Peace Corps that they will be charging the Peace Corps for services they performed during the pilot program, the estimation for these charges is approximately \$24,000. The reasoning for this charge is unclear and the Peace Corps is currently negotiating the amount it is willing to pay. However, since the existing MOU was not signed by the chief acquisition officer, the Peace Corps will be required to create a new agreement with the proper authorization to pay for these reimbursements, once the Peace Corps agrees to a payment amount.

### **Proper Offices and Staff Have Not Been Involved**

While a decision on which cloud provider to use agency-wide was expected in mid-February 2015, as of December 2014 many critical offices and staff were not consulted to ensure the cloud solution would meet the required federal laws and requirements. The Peace Corps Office of Management has been working to address mandates from an Office of Management and Budget memorandum, M-12-18, that requires federal agencies to manage all permanent records in electronic format by 2019 and all permanent and temporary email records in electronic format by 2016. In May 2014, the Office of Management was granted a request for additional resources to develop an agency-wide electronic management system. However, staff responsible for this effort had not been consulted or asked to evaluate whether any of the existing cloud technology solutions would provide adequate controls to address this federal requirement.

In addition, as of December 2014, no IT security staff had been asked to perform a review of the security controls provided by any of the cloud technology solutions. The former CIO expressed that she wanted to perform a security assessment of Google Apps prior to launching the cloud pilot program, but was told by other members of the cloud implementation team that this pilot was a high priority and there was not time to perform this analysis.

In October 2014 the cloud implementation team developed an evaluation strategy document as a tool to determine whether the Peace Corps should implement Google Apps agency-wide or pursue an alternative cloud service provider. In this document, the criteria to evaluate these solutions are broken out into two categories: primary and secondary (see Appendix 3 for a list of the evaluation criteria). Our review of the strategy disclosed that alignment with federal policy is only a secondary criterion. Moreover, it is unclear if the strategy incorporates records retention requirements. We note that the evaluation criteria does include “can the platform can integrate or support edge cases (i.e., China).” As of December 2014, many news reports cite that China banned the use of Google’s email application. It is important that the agency consider how this post will be included in the future infrastructure if Google is selected as the cloud provider for agency-wide implementation.

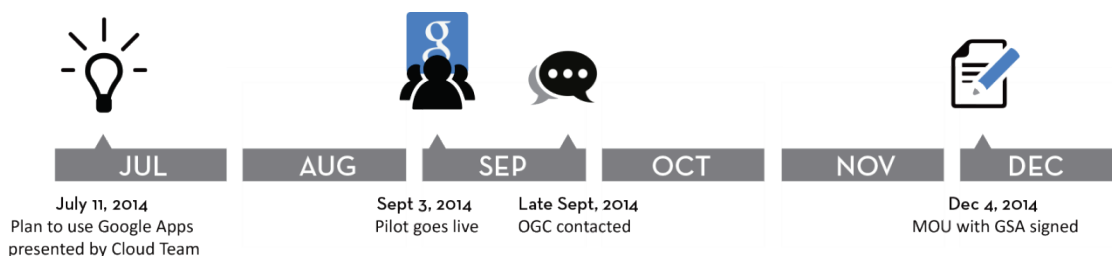
Involvement of all the primary stakeholder offices throughout the process is critical to ensure that a permanent cloud provider can meet all federal and agency requirements. Furthermore, the lack of office involvement during the pilot program has created an unnecessary risk that the selected cloud provider will not be able to meet the agency's needs.

### **Agreement with GSA Not Adequate**

The cloud pilot program ran without any controls in place for three months until the MOU with GSA was signed in December 2014. An MOU is the Peace Corps' only control mechanism to ensure the Peace Corps receives the services and goods promised. Transferring sensitive agency information, potentially including personally identifying information (PII), to GSA and the Google cloud without a basic agreement in place put the agency at risk. This problem is further compounded by the fact that the Peace Corps did not review a copy of GSA's agreement with their cloud provider, which provides the underlying basis for how Peace Corps data is treated.

Furthermore, the Office of General Counsel (OGC) was not contacted to work on developing an agreement with GSA until late September 2014; over two months after a decision on the pilot approach and after live data was transferred to the cloud (see Figure 1 for a timeline of these key dates).

**Figure 1. Key Dates Related to MOU**



Without a strong MOU with the providing agency there are no assurances that our information is being properly handled and protected. On July 22, 2014, OIG expressed the need for the agency to establish an agreement with GSA and raised concerns to the general counsel and the former CIO on access, ownership, location, and security of data needed to be addressed to protect agency information; but these concerns were not incorporated into the MOU because members of the cloud implementation team considered the data risks were minimal because the program was only a pilot. All incoming emails are first captured at Peace Corps and then replicated out to the Google Apps environment. However, any response a pilot participant sends from Google Apps is not captured at Peace Corps and therefore there is not a copy saved with the pilot participant's regular email account. Furthermore, any document created or edited in the shared collaboration space is not stored within Peace Corps systems. These documents only live in the Google Apps environment and maybe official government records.

The MOU did not define who at GSA may access Peace Corps data or how any third parties would get access to records if needed. For example, criminal cases, electronic discovery, or a subpoena for information could be served to the Peace Corps and the agency would need to produce the electronic records. However, many U.S. based companies and federal agencies have experienced problems with getting access to their own information if it is being stored outside

the U.S., since other countries have different laws on the jurisdiction for access. There is no provision in the MOU with GSA requiring our information be stored in the U.S.

Neither the MOU nor the pilot addresses how information is stored and protected, as well as how data and media are destroyed or, if legally required, transferred to the National Archives and Records Administration (NARA) for permanent retention. The Peace Corps has established records retention requirements that have been legally approved by NARA. Since document collaboration is part of the Google pilot program, it is critical for these records to be preserved, properly managed, and then destroyed or, if legally required, transferred to NARA, all in accordance with the established records schedules. It is also important to state that emails are records as well and as such, they must also be preserved, managed and destroyed or, if required, legally transferred to NARA. Furthermore, there are federal requirements that any breaches or loss of government information must be reported to the Department of Homeland Security; however, the MOU does not include a definition of who is responsible and how this breach or loss would be reported and more importantly, how the situation would be mitigated and resolved. By moving forward in this manner, the Peace Corps risks non-compliance with federal laws and regulations.

The Peace Corps' apparent decision to move to Google Apps as the final agency-wide cloud platform is illustrated by its lack of an exit strategy in the MOU. While the MOU states that the Peace Corps is not obligated to enter into a long term agreement with GSA, there are no terms by which Peace Corps can terminate the agreement. Specific associated costs, procedures, and timelines have not been identified.

Since the MOU lacks basic controls and key terms such as ownership of data, access to Peace Corps information, and data security, reviewing the actual agreement between GSA and its cloud provider Unisys is critical. By signing the MOU Peace Corps is allowing its data to be handled according to the terms and conditions found in the agreement(s) between GSA and Unisys.

The Federal Risk and Authorization Management Program (FedRAMP), the government-wide program that provides a standardized approach to security for cloud products and services, developed the policies and standards for cloud providers in December 2011. However, GSA developed its statement of objectives and request for cloud service providers in June 2010, a year and a half prior to when these policies and standards were developed. The GSA contract could have been modified to ensure these subsequent security standards were followed, but the Peace Corps has not conducted its due diligence in either reviewing the contract or including key terms in their own MOU with GSA. Therefore, the Peace Corps has no assurance that its data is being properly protected.

### **IT Security Controls Lacking**

The Peace Corps did not view information security as a key priority during the implementation of the pilot program. Almost a month after the cloud pilot program was launched; a risk acceptance waiver was signed stating that OCIO would *not* be completing the standard security assessment and accreditation process normally conducted prior to granting the authority to operate a new IT platform. This full assessment was not conducted to avoid a delay of implementing the pilot and reduce the costs of engaging information security analysts. The risk

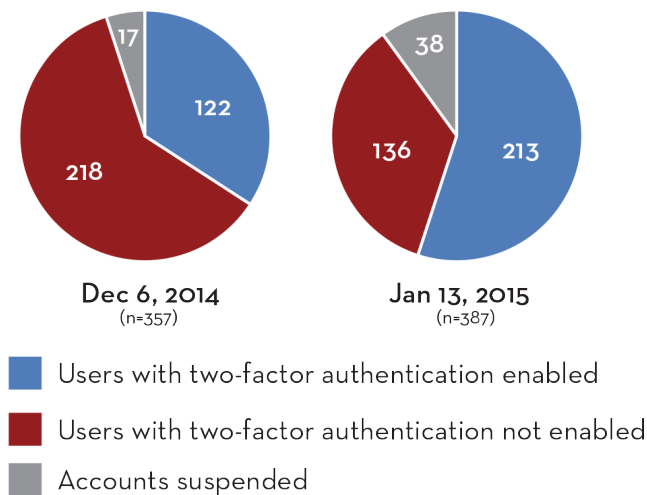
acceptance waiver outlined only three known security risks, but admitted there could be others that would remain unknown. Since the agency did not conduct an IT security assessment as requested by the former CIO, there is no way for the agency to identify and mitigate other security risks. We believe this level of risk acceptance is unprecedented in the federal information system risk management community. The risk acceptance is even more remarkable given that IT security has been determined to be an agency-wide management and performance challenge for at least 10 years.

One of the known risks identified was the settings for two-factor authentication and that having this feature enabled was not the default for the Google platform. The risk acceptance waiver stated that users must individually elect to turn this feature on. However, through interviews with the cloud implementation team, we learned that the two-factor authentication feature could have been set up for the overall platform and did not need to be pushed down to the user level to set up. The mitigating controls established in the risk acceptance waiver were to provide users training on setting up two-factor authentication and then suspending accounts that did not have this feature enabled. However, as of December 6, 2014, 218 of 357 pilot users had not set up two-factor authentication and only 17 accounts had been suspended.

On December 11, 2014, we requested information on how many accounts had been suspended and how many users had not turned on two-factor authentication, as well as documentation on the process to train users. The cloud implementation team provided many instances where two-factor authentication was mentioned or directions were provided. Guidance was also included in the initial implementation training for all new pilot users; however, there was no communication from the cloud implementation team to users alerting them that their accounts would be suspended if this feature was not enabled. Additionally, the only communication requiring users to set up two-factor authentication was issued to users on December 11, 2014, after we made this request for information; 11 days after the pilot program was scheduled to be completed. However, we note that the cloud implementation team had some success in getting users to turn on two-factor authentication subsequent to their December 11 communication. As of January 13, 2015, 136 users had not enrolled in two-factor authentication, a reduction of 82 from the 218 who had not previously enabled this feature. There were also an additional 21 accounts that were suspended (see Figure 2 for a graphical illustration of the enrollment).



**Figure 2. Two-Factor Authentication Enrollment**



We also learned that two-factor authentication as applied to Google pilot platform has serious problems. Google pilot users using two-factor authentication have the ability to select to stay signed in for 30 days, while this option is not available to users who do not have two-factor authentication turned on. Two-factor authentication can be a mitigating factor; however, as applied currently it places Peace Corps information at further risk. For example, if a user selected two-factor authentication and the option to stay signed in on a public computer, all Peace Corps emails and document collaboration associated with that user account would be available to any outside individual for up to 30 days. Furthermore, the cloud implementation team does not have a way to monitor or identify which users have elected to stay signed in with this method of two-factor authentication.

We also have concerns about the general state of the Peace Corps IT security situation. While moving to the cloud does remove some of the direct IT burden for OCIO, it also puts a large responsibility on establishing a robust service level agreement with the cloud provider and strong IT security controls to ensure that information is adequately protected. It is important to note that the Google Apps solution has not been certified as an approved cloud provider under the FedRAMP process as of January 2014.

### **Conclusion**

We support the agency's desire to move to a cloud infrastructure and believe this will help Peace Corps modernize, be more efficient, and improve the agency's infrastructure, but it is critical that this innovation be done with careful planning and considerations of all needs of the agency. In order to successfully leverage a cloud-based solution, the process to select a provider needs to be thoroughly planned, vetted, and tested to ensure cost savings are met, federal laws and requirements are addressed, security controls are strong, and all options are properly considered.

**We recommend:**

1. That the cloud implementation team terminate all pilot users from the Google Apps cloud pilot.
2. That the cloud implementation team, in conjunction with Office of Management, work to ensure any official agency records generated during the Google Apps pilot be correctly stored and destroyed according to the Peace Corps' records schedule.
3. That the cloud implementation team identify comprehensive requirements for a cloud technology solution. This effort should include input from Office of the Chief Information Officer, Office of Management, and analysis of all required federal requirements and laws.
4. That after the comprehensive requirements are identified, the cloud implementation team work with the chief acquisition officer to identify the best acquisition approach for obtaining the cloud technology solution.
5. That the Office of the Chief Information Officer perform a full IT security assessment on potential cloud based systems prior to transferring Peace Corps data to the systems.
6. That the Director ensure that all agreements the Peace Corps enters with any cloud service provider be fully documented and all key terms such as ownership of data, access to Peace Corps information, and data security be outlined.

cc: Laura Chambers, Chief of Staff  
Jacklyn Dinneen, White House Liaison  
Rudy Mehrbani, General Counsel  
Joseph Hepp, Chief Financial Officer  
Francisco Reinoso, Chief Information Officer  
Dorine Andrews, Senior Advisor to the CIO  
Vince Groh, Deputy Chief Information Officer  
Carlos Torres, Associate Director, Global Operations  
Shelia Campbell, Director of Digital Integration  
Patrick Choquette, Director of Innovation  
Garry Stanberry, Deputy Associate Director, Management  
Valery Garrett, Records Management Officer, Management  
Linda Brainard, Chief Acquisition Officer  
Anne Hughes, Deputy Chief Compliance Officer  
IGChron  
IG

Appendix 1: Risk Acceptance Waiver

Appendix 2: MOU with GSA

Appendix 3: List of Evaluation Criteria from Evaluation Strategy Document



Since 1961.

September 19, 2014

**RISK ACCEPTANCE WAIVER**  
**CLOUD EMAIL PILOT WITH GSA**

---

**Background:**

Peace Corps is evaluating cloud-based platforms for providing email and document collaboration tools to staff and potentially Volunteers. The agency has entered into an inter-agency agreement (IAA) with the General Services Administration (GSA) to pilot GSA's cloud solution based on Google Apps for Government. The pilot will run from September 3, 2014 through December 31, 2014. It will include ~250 participants selected from headquarters offices and overseas posts. Participants will be using the pilot cloud platform for drafting, sending and saving normal emails and documents relevant to their work. By the end of the pilot, Peace Corps intends to make a decision to (1) migrate to GSA's Google Apps solution, (2) migrate to another cloud-based email platform, or (3) postpone the migration.

To allow Peace Corps to quickly commence the pilot, OCIO will not complete the standard security Assessment and accreditation (A&A) process normally conducted prior to granting an Authority to Operate (ATO) approval required for a new IT platform. Not completing this A&A process will avoid a delay to the pilot of several months and will avoid the costs of engaging information security analysts in a significant security review of a system used potentially for only a few months. This A&A process will be conducted if Peace Corps chooses to move the entire agency to the Google Apps platform.

Peace Corps staff, particularly members of the security and technology operations teams, have evaluated the solution provided by GSA for the pilot and are aware of several security concerns. In some cases, these concerns have already been mitigated; in other cases, the pilot is operating with known security risks and concerns. During the pilot, Peace Corps will evaluate each of these risks and identify solutions if the GSA Google Apps platform is selected for deployment across the entire agency.

The known specific security concerns with the pilot Google Apps platform as configured for the pilot are:

- 1) When users authenticate to Google Apps they are given the option to "stay signed in" which will allow them to skip the authentication process on subsequent sessions. Federal standards stipulate that systems be designed to require re-authentication after 30 minutes of inactivity. This is a known concern with Google Apps and GSA has formally accepted this risk for their implementation of Google Apps. [Pilot participants have been trained to select "stay signed in" only on trusted work or personal computers that require a separate authentication to access; pilot participants should not select "stay signed in" when using a public or shared computer, e.g. internet café. This is the standard guidance for Google Apps.]
- 2) Google Apps provides an option for two-factor authentication (username/password plus a code sent to a separate device via SMS); however this is not the default and users must elect to set this feature. Federal standards require two-factor authentication for all remote access. For the pilot, participants will be trained to set up two-factor authentication in the Google environment.

Additionally, reports will be produced to identify pilot participants who have not established two-factor authentication; after a warning, these accounts will be disabled.

- 3) During the pilot, users will be able to access their Google Apps account from personal mobile devices. This access does not conform to Peace Corps' current policy for personal device usage (e.g. Peace Corps will not be able to delete agency data from devices reported lost or stolen, data is not encrypted on personal devices). If Peace Corps deploys Google Apps for Government to all agency staff, changes to the personal device usage policy and procedures will be required.

Additional risks may be present in the pilot configuration of Google Apps—because a full security analysis will not be conducted for the pilot, those risks may remain unidentified.

**Risk waiver Acceptance:**

Peace Corps will execute the pilot of Google Apps for Government with GSA with the above identified security risks with ~250 participants using normal work-related emails and documents (information defined as *low* or *moderate* risk) from early September through December 31<sup>st</sup>. The tool will not be used for communications requiring "Top Security" and "Security" position clearances. If Google Apps for Government is selected as Peace Corps cloud email platform during the pilot, this waiver may be extended beyond December 31<sup>st</sup> 2014 until the official launch to avoid disruptions to pilot participants.

☒ Approved    ☐ Not Approved



Dorine Andrews, Chief Information Officer

9.29.2014

Date

☒ Approved    ☐ Not Approved



Kathy Rulon, Agency Risk Executive

9-25-14

Date

MOU GSA IT/Peace Corps Cloud Email Pilot

**MEMORANDUM OF UNDERSTANDING**

between  
GSA IT  
and  
Peace Corps

**SUBJECT:** Cloud Email Pilot

**1. Overview.**

This document outlines the General Services Administration (GSA) GSA IT plan to provide Cloud Email Pilot Service to the Peace Corps, and anticipates the period of performance for this effort to be from date of last signature on this document through 30 May 2015, (FY14-FY15). During this project there are contracts and services that GSA will pay for in phase 1 and 2 for the Cloud Email Pilot. The Economy Act gives GSA the authority to perform this service for the Peace Corps.

The Peace Corps Cloud Email Pilot Service, at a high level, is a three (3) phase approach:

**Phase 1: Basic Pilot for Organizational communities and members of the Organization.**

The first phase will test the different site configurations for software warranty to meet the various Peace Corps demands and requirements. It is a test of the "Line of sight" from Headquarters to Region to Country to Post and will confirm if the software will meet Peace Corps requirements and functionality. Both the GSA and Peace Corps will work together to develop a blueprint for transitioning to Cloud Email Services which will include use cases for headquarters (HQ), regional, country, and field office scenarios with high bandwidth, and low bandwidth remote site environments. The Peace Corps will consult with GSA and end users to define tests needed to best ensure a complete picture of what the challenges are in preparation for the Peace Corps implementing Cloud Email across the agency. The pilot will broaden the existing email community from Government only to include Peace Corps Volunteers.

**Phase 2: Extend Phase 1 Pilot to Communities with Peace Corps Subject Matter Experts receiving Train-the-Trainers training and supporting the Communities as PACERS**

The second phase will extend the pilot and focus on creating Peace Corps Subject Matter Experts who will be trained to be trainers to support the Peace Corps Communities as "PACERS". This will be a mix of currently active members as well as new candidates.

## MOU GSA IT/Peace Corps Cloud Email Pilot

Phase 1 and 2 has a budget, paid for by GSA, of \$100,000.00 that will augment existing staff and contractor support of GSA. The budget can also be used to obtain smart tools for the Peace Corps including mobile devices, coordination with local cell providers, licensing, change management/training and travel. The goal is to establish a core group within the Peace Corps called PACERS to perform Train-the Trainer in Phase 2 in preparation for Phase 3 enterprise deployment.

### **Phase 3: Enterprise delivery - Rollout to all communities, "GO LIVE" or "ROLL BACK".**

Phase 3 is the Peace Corps enterprise-wide transition to Cloud Email for operations and maintenance or a return to the existing environment. The intended goal of Phase 3 is to support the Peace Corps' decision based on the assessment of Phase 1 and 2 of the Pilot. If the decision is to continue, phase 3 would move quickly using PACERS to share, collaborate and connect for the cloud extended Pilot across the enterprise. If the result of the pilot is not to continue, GSA will work with Peace Corps to revert back to the original environment. GSA is a shared service email provider for the government, and has not only the tools and experience, but is prepared to support and assist Peace Corps with economical cloud solutions for quick cloud email transition.

Again, no matter what the decision, Phase 3 is not part of this MOU and will not proceed without a signed SF7400 A and SF7400 B. Phase 3 will be detailed in a separate agreement with costs reimbursed to GSA by the Peace Corps at an agreed amount for support and service. It may include but not be limited to Mobile Devices and Management, Help Desk, Risk Management, Travel, Licenses, Products, Change Management, and Operations and Maintenance. It could include full agency deployment or a return to the previous environment and is provided as a cost reimbursable service by GSA.

The following services are available in Phase 3 but separately priced: archive and historic email preservation services; transitioning or decommissioning existing services; roll back to previous mode of operation for email communications.

As stated above, nothing in this MOU or by virtue of Peace Corps and GSA's participation in Phase 1 or 2 shall obligate Peace Corps or GSA to enter into a separate Agreement for Phase 3.

Whatever decision is made as a result of Phase 1 and 2 of the Pilot, the goal is a business decision for a solution that results in a fast transition to a cloud environment for email services that result in cost savings, collaboration and increased use of shared services. GSA's mission is to make this happen for the Peace Corps.

## **2. Scope of Work.**

In providing this Cloud Email Pilot Service, GSA will:

1. Provide end-to-end support for pilot cloud-based email services in the following manner;
2. Provide a list of GSA points of contact (POC) with their email and telephone information;
3. Work with Peace Corps to develop a Mobile Device Management Governance to support both Government Supplied Devices and Bring Your Own Devices;
4. Identify and provide limited number of mixed mobile devices (smart technologies) in accordance with agreed Blueprint and Governance;
5. Provide technology devices for Peace Corps pilot in accordance with agreed Blueprint for Cloud Services, as necessary;
6. Provide licensed access to the cloud email (Google Apps NTE 500 Licenses) software and collaboration tools during the time periods identified and as described in the deliverables section; according to the negotiated pricing in Infrastructure as a Service, at no cost to the Peace Corps.
7. Stand up the new domain peacecorps.gov and transfer up to 500 GSA licenses to the new domain based on staging definitions to be found in the Project Blue Print;
8. Provide analysis for low-bandwidth usability;
9. Provide system administration for the software during the time periods identified in the deliverables section to include establishing the environment and accounts;
10. Provide the hardware support (any device, anywhere, anytime), associated hosting and connectivity for the software during the time periods identified in the deliverables section;
11. Provide the Change Management Plan, Training Plan and Training Material;
12. Work with Peace Corps to identify and quantify Technology Performance Measures and assist the Peace Corps in developing an overall Evaluation Strategy for the pilot based on Peace Corps' requirements;
13. Work with Peace Corps to maintain existing Risk log and ongoing risk assessments. As an outcome of the risk assessment effort, identify the potential Risks (Threats and Opportunities) and work with Peace Corps to develop the corresponding Risk Mitigation strategies;
14. Provide acquisition options to support the Peace Corps' long term requirements with Cloud-based email;
15. Assist Peace Corps staff to establish a FAQ section to use during the Cloud-based email pilot and thereafter for enterprise use;
16. Deliver training sessions for pilot participants that, in collaboration with Peace Corps Cloud Pilot team members, have clear learning objectives;
17. Provide weekly data reports to Peace Corps to assess usage rates, compliance with two-step verification, and other key indicators;

**MOU GSA IT/Peace Corps Cloud Email Pilot**

- 18. Assist in setting up and participating with Peace Corps on the Executive Board for project oversight that will provide executive guidance and oversight related to the Google Cloud-based email.**
- 19. Conduct Lessons Learned with Peace Corps and teams throughout each phase and produce Lessons Learned White Paper at the end of each phase set forth in 2(b) below, addressing metrics and successes, risks and risk management, best practices and initial project Rough Order of Magnitude (ROM) (i.e., cost estimate) and initial Return on Investment (ROI). This will be further refined as the Phases progress;**
- 20. Provide the Executive Board with recommendations from the PMO for "Go/No Go" and/or Roll-Back Strategies.**
- 21. Per Peace Corps direction provided to GSA, maintain all information security requirements during all aspects of the Cloud-based Email Pilot Services to the appropriate levels required by Peace Corps in accordance with federal laws applicable to federal agencies effective during the pilot.**

**In acquiring these pilot cloud-based email services, Peace Corps will:**

- 1. Provide a list of Peace Corps points of contact (POC) with their email and telephone information for project coordination;**
- 2. Work with GSA on the Blueprint for Cloud Services;**
- 3. Provide the naming convention for Peace Corps email user names;**
- 4. Put out a call for PC offices interested in participating in the pilot across Peace Corps;**
- 5. Work with GSA on the analysis of the respondents interested in participating in the Pilot;**
- 6. Provide the list of pilot participants who will be available for the complete duration of the pilot;**
- 7. Bring the Peace Corps communities together virtually for participation in the pilot – training, change management, implementation and deployment;**
- 8. Support and Conduct Phase 1 pilot for the agreed to time frames;**
- 9. Work with GSA to monitor pilot progress and collect lessons learned from participants;**
- 10. Provide and provision any technology devices for Peace Corps pilot beyond the agreed upon Blueprint;**
- 11. Provide timely communications with GSA for support and services;**
- 12. Work with GSA to develop and execute Mobile Device Management governance to support the pilot;**
- 13. Work with GSA to identify Risks and Risk Mitigation strategies;**
- 14. Work with GSA to deliver training sessions for pilot participants, in collaboration with Peace Corps Cloud Pilot team members, and identify core learning objectives;**
- 15. Work with GSA to Establish an Executive Board for governance, oversight and direction of the Cloud Email Program within the Peace Corps; and**
- 16. Take the lead and coordinate any audits/ reviews related to this specific requirement.**



# MOU GSA IT/Peace Corps Cloud Email Pilot

Peace Corps shall retain ownership of all data created and stored in the Cloud-based Email Pilot including but not limited to all emails, all documents developed or stored in Google Doc, and calendar entries created during the pilot program. GSA has provided user licenses for the purposes of the Pilot.

**3. Deliverables.** Table 2 outlines the proposed GSA deliverables.

The proposed deliverables are based on Phase 1 and 2 having a six (6) week staging period and being conducted during September 2014 – March 2015. Phase 1 will support communities of subject matter experts of approximately 300 virtual users. Phase 2 will support communities of Train-the-Trainers of approximately 200 additional users for a not to exceed total of 500 licenses. Phase 3 which supports all communities is anticipated to follow Phase 2.

The estimate of deliverables is based on the current known schedule and projections at the time this document was produced. Changes to the schedule may require changes to the deliverables and costs and would be a modification to this MOU.

**Table 2. Deliverables**

Description	Price	FY14 + FY15	Cost GSA	Cost Peace Corps
Phase 1&2 GSA will as detailed in section 2: a) Provide end-to-end support for Cloud Email Pilot Services including FISMA and any other applicable federal security requirements per direction from Peace Corps during the pilot b) Provide expert support for the Cloud Email Pilot Services for the Peace Corps Phase 1 and 2 c) Travel & Other Direct Cost	\$100,000.00	2	\$100,000.00	\$0.00

**MOU GSA IT/Peace Corps Cloud Email Pilot**

Peace Corps will: a) Support items a and b above, as detailed in section 2				
Phase 3 TBD in a separate Agreement	tbd	1	\$00.00	tbd
<b>Total</b>	<b>\$100,000.00</b>	<b>-</b>	<b>\$100,000.00</b>	<b>\$00,000.00</b>

**4. Assumptions.** The GSA has made several assumptions, detailed below, in developing this cost estimate. If these assumptions are not valid, the cost estimate may require modification.

- a. The GSA will provide the services for Phase 1 and Phase 2 at no cost to the Peace Corps. Phase 3 "GO LIVE" or "Go Back" funding will be received from the Peace Corps prior to work starting and based on a negotiated amount for services.

**Note:** Nothing in this MOU or by virtue of Peace Corps' participation in Phase 1 or 2 shall obligate Peace Corps to enter into a separate Agreement for Phase 3.

**PHASE 1 & 2:**

- a. If the actual costs are less than estimated, the difference may result in remaining funds. These funds can be reallocated to the project by GSA with the understanding they may not be fully consumed.
- b. If any item identified in the deliverables (Table 2) is not provided during the period identified in the schedule (Table 3), due to unanticipated delays such as those listed in the assumptions, the items will be reallocated to Phase 3 and costs re-evaluated.
- b. The Peace Corps program points of contact or the program manager identified in this agreement will provide a completed user profile for each user requiring access one (1) week prior to user access to the GSA technical points of contact.
- c. The pilot project will be conducted in English (no other language support will be required by Peace Corps). The Peace Corps will provide support for any local language, politics, and change management if needed for the success of the pilot.
- d. The Peace Corps will coordinate their staff schedules and ensure availability of participants during the pilot.

MOU GSA.IT/Peace Corps Cloud Email Pilot

- e. Due to the dispersed geographical nature of the pilot, unanticipated implementation delays due to act of God, terrorism, evacuation and /or war, or natural disaster will not extend Phase 1 and/or Phase 2 but could result in the Peace Corps revising Phase 3 support services.

**5. Schedule.** Table 3 identifies the support/delivery schedule for deliverables identified in Table 2.

**Table 3. Schedule**

<b>GSA –email Services</b>	<b>Start</b>	<b>End</b>
Phase 1	9/3/2014	12/1/2014*
Pilot Evaluation Assessment 1	12/1/2014	12/31/2014
Phase 2	01/15/2015	03/15/2015*
Pilot Evaluation Assessment 2	03/01/2015	03/31/2015
Phase 3	TBD	TBD

\*NOTE: Pilot participants will continue to be supported through the Assessment Period which will conclude with the "Go / No Go" decision on or before the end evaluation assessment date listed in Table 3. If in a Go they will be continued into the next phase or No Go returned to the pre-pilot environment.

**6. Funding Responsibility.**

The Peace Corps Program Office will not be responsible for funding any of GSA's approved expenses (e.g., labor, travel, etc.) on a cost reimbursable basis unless Phase 3 is implemented. Phase 1 and Phase 2 are at no cost to the Peace Corps and are not to exceed \$100,000.00 expenditure by GSA. The \$100,000.00 expenditure does not include GSA's Full Time Equivalence (FTE) expenses which also shall be borne by GSA.

Projected funding and resource requirements are based on the currently stated requirements. Changes in any of these areas, or other influences outside the control of GSA or the Peace Corps, will require advanced approval for additional funding to continue required support.

Nothing in this MOU or by virtue of Peace Corps' participation in Phase 1 or 2 shall obligate Peace Corps to enter into a separate Agreement for Phase 3.

**7. Funding Requirements.** Table 4 contains the anticipated funding requirement that GSA will bear to support this effort.

**Table 4. GSA Funding Requirements**

<b>Cost Category</b>	<b>FY-14</b>	<b>FY-15</b>
Labor	\$0.00	\$00,000.00
Deliverables, Travel, ODCs, Devices, Contact Support e.g. ISP Service	\$100,000.00	\$0,0000.00
Total Estimate	\$100,000.00	\$00,000.00

**8. Funding Information:** Phase 1 and 2 will be funded by GSA and this MOU does not have a funding transfer associated with those expenses

**9. Disputes:**

Disputes related to this MOU shall be resolved in accordance with instructions provided in the Treasury Financial Manual (TFM) Volume I, Part 2, Chapter 4700, Appendix 10; Intragovernmental Business Rules.

**10. Termination:**

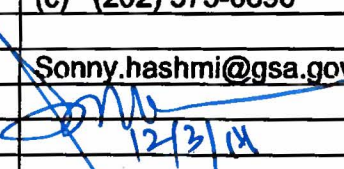
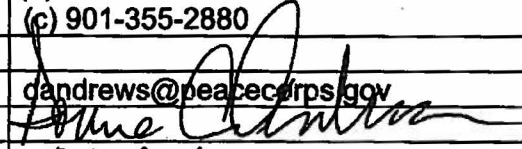

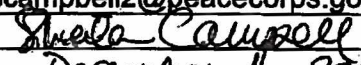
This MOU may be terminated by 30 days' written notice by either the Requesting or Servicing Agency.)

If this agreement is canceled, any implementing contract/order may also be canceled. If the MOU is terminated, the agencies shall agree to the terms of the termination, and each party agrees to bear its own costs associated with cancellation.

MOU GSA IT/Peace Corps Cloud Email Pilot

**11. Approvals and Points of Contact:**

Program Officials:

	GSA	Peace Corps
Name	Sonny Hashmi	Dorine Andrews
Title	GSA CIO	Peace Corps CIO
Telephone Number	(o) (202) 681-1241 (c) (202) 573-0896	(o) 202-692-1300 (c) 901-355-2880
Fax Number		
Email Address	Sonny.hashmi@gsa.gov	dandrews@peacecorps.gov
Signature		
Date Signed	12/3/14	12.1.2014
Name	Mary Davie	Sheila Campbell
Title	Asst. Commissioner for Integrated Technology Services	Peace Corps Director of Digital Integration
Telephone Number		202-692-1042 Office 202-413-3789 Cell
Fax Number		
Email Address	Mary.Davie@gsa.gov	scampbell2@peacecorps.gov
Signature		
Date Signed	12.4.14	December 11, 2014

Additional POC:

Role	Information	GSA	Peace Corps
PMO	Name	Earl Warrington	Sheila Campbell
	Title	Assistant Deputy Associate Administrator Office of IT Services & Solutions Office of Citizen Services and Innovative Technologies (X)	Director of Digital Integration Peace Corps
	Office Phone	(o) 202-208-6158	202-692-1042
	Cell Phone	(c) 703-856-6925	202-413-3789
	Email:	earl.warrington@gsa.gov	Scampbell2@peacecorps.gov

**MOU GSA IT/Peace Corps Cloud Email Pilot**

**The Interagency Agreement should be emailed or faxed to:**

**GSA  
ATTN: Earl Warrington  
Address: 1800 F St NW  
Washington, DC 20405-0001  
Fax: call first  
Email: earl.warrington@gsa.gov**

**Provide any comments or concerns regarding GSA's support on this program to:**

**Mike Seckar  
Deputy Associate Administrator CIO  
(o) 202-208-5054  
(c) 703 – 906-9545  
Mike.seckar@gsa.gov**

**List of Criteria from the Evaluation Strategy for the Cloud Email and Collaboration Pilot**

Criteria	How We'll Measure	Google Apps	MS 365	Current State
<b>Primary</b>				
Functionality	Matrix of key features (see Addendum)			
User satisfaction	User surveys and focus groups			
Familiarity and preference	-- % of our target user base who already use the platform -- # of users using tool worldwide			
Cost	licensing fees; cost over 5 yrs for staff and Volunteers			
User autonomy, flexibility, and mobility	Does platform give users maximum flexibility to collaborate and share anywhere, anytime, on any device?			
Mitigation of security and other risks	Does platform conform to FISMA, FEDRAMP, disaster recovery, data ownership requirements			
Community-based and DIY technical support	Size of user support community; availability of DIY resources			
<b>Secondary</b>				
Alignment with federal policy (open data, open source, shared service, cloud first)	Is product open source? cloud-based? consistent with open data principles? Modular? Is the platform extensible through open APIs?			
Scalability and innovation	What is the rate of innovation for the application? How quickly does platform evolve and iterate based on user feedback?			
Performance / reliability	SLAs; performance at low bandwidth posts			
Integration	To what extent can platform integrate with current and future systems? Can the platform integrate or support edge cases (ie China)?			