Office of Inspector General

APR 13 2012

MEMORANDUM FOR THE ADMINISTRATOR

FROM: Michael G. Carroll
Acting Inspector General /s/

SUBJECT: Risks Associated with Using Cloud Computing Services

Cloud computing[1] creates new information technology opportunities by offering the promise of cost savings combined with increased agility. For example, cloud computing providers already offer users of various types of devices, including personal computers, laptops, tablets and smart phones, the opportunity to access programs, storage, and processing over the Internet. Nonetheless, cloud computing also presents risks, particularly for federal agencies which face policy concerns and regulations that may differ from the private sector.

Cloud computing does not lend itself to easy generalities. Vendors and applications vary widely. Some reputable, well-established cloud vendors could be entrusted with very sensitive information, while some marginal vendors should not be entrusted even with less significant data. Some applications are very well suited to migration to the cloud, while policy considerations militate strongly against moving other applications to the cloud.

As an example, the OIG has concluded that our most sensitive law enforcement records fit into the latter category. Transition to the cloud is inappropriate. Other USAID components may identify similarly sensitive applications.

[1] Simply defined as: "Hosting data or applications on pooled remote servers accessible via the Internet." Essentially, cloud computing is a way of outsourcing some IT services, to take advantage of economies of scale.

U.S. Agency for International Development
1300 Pennsylvania Avenue, NW
Washington, DC 20523
www.usaid.gov/oig

In the attached report, Audit of USAID's Contracts for Cloud Computing Services, we concluded that USAID's contract clauses did not address the following control areas (Tab1):

- Data Security
- Application Security
- Compliance and Audit
- Asset Availability
- Maintenance
- Intellectual Property
- Incident Response
- Legal and Electronic Discovery
- Termination and Transition
- Portability and Interoperability

As a result of not addressing the aforementioned control areas in the contract clauses, USAID is potentially at risk of not securing its data and assets. Moreover, this affects the confidentiality, integrity, and availability of USAID's information.

As a proactive measure, OIG is providing additional risk factors for your consideration and to assist USAID in implementing a solution that is secure, reliable and cost-effective (Tab 2). While OIG recognizes that cloud computing is a relatively new technology and that the related risks and best practices for controls are still emerging, we believe USAID should provide assurance that all significant risks have been thoroughly considered and that all possible steps have been taken to mitigate those risks and comply with all applicable policies, standards, and regulations.

If you have any questions or wish to discuss this document further, I would be happy to meet with you.

Attachments:

Tab 1: Audit of USAID's Contracts for Cloud Computing Services
Tab 2: Potential Risk Associated with Cloud Computing at U.S. Agency for International Development

The U.S. Agency for International Development Office of Inspector General (OIG) is withholding from public release Tab 1, *Audit of USAID's Contracts for Cloud Computing Services*. This report contains sensitive but unclassified (SBU) information, the disclosure of which would risk the integrity of agency information systems.

This audit report, number A-000-12-004-P, was issued April 12, 2012 by OIG Office of Audit's Information Technology Audits Division. OIG publicly disclosed the report's issuance in its Semiannual Report to the Congress, April 1–September 30, 2012, which contained the following information from the audit report:

> *OIG conducted this audit to determine whether USAID's contracts for cloud computing services included best practices and controls. OIG found that, of the 11 best practices and control areas selected for review, only one was included in its entirety in both contracts. OIG made seven recommendations to improve the Agency's contracting practices and controls for cloud computing services, and management decisions have been made on all of them.*[1]

[1] Semiannual Report to the Congress, April 1–September 30, 2012, p. 50; http://oig.usaid.gov/sites/default/files/other-reports/sarc0912_0.pdf

Tab 2

POTENTIAL RISK ASSOCIATED WITH CLOUD COMPUTING AT U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT		
	Description	**Risks**
1.	**Data Security** provides protection of agencies' data and information.	• Data stored on cloud provider's servers may be physically located anywhere in the world and may not be protected by U.S. laws. • Foreign governments or terrorists could access, modify or disclose USAID sensitive data. • Data may be unencrypted when in transit or stored on vendor's servers, which increases the risk that USAID's data could be exposed to unauthorized use and released without proper authorizations. • Response to security incidents may be untimely and require long periods of time to bring the systems back on-line and re-secure after outages. • Access to backup data may not be limited to authorized persons and vendors' access or use of USAID's data may not be prohibited. • Sensitive and restricted law enforcement data could be distributed to unauthorized persons.
2.	**Application Security** provides protection of USAID's systems such as Phoenix and GLAAS, which is based on the risk and magnitude of harm or unauthorized access or modification of the information in the system.	• Application software that is running in the cloud could be at risk of unauthorized access, data leakage, and system unavailability.
3.	**Asset Availability** gives agencies the ability to continue their business operations and meets their needs when the cloud provider implements new software and hardware for compatibility, software updates, hardware refresh, and maintenance.	• Without disaster recovery and business continuity plans in place, USAID's business processes may be impaired if access is unavailable. • Incompatible hardware and software upgrades could result in costly solutions and long response time to address system outages and disruption of business operations. • Untimely and uncoordinated software updates and hardware refresh could significantly impact agency's operations. • Unavailability of law enforcement information/data may not meet judicial and congressional demands. (Instant availability of usable, uncorrupted, untainted data is a business necessity.)
4.	**Monitoring and Tracking Flow of Data** are used by agencies to monitor and track network traffic and data. Usually, monitoring tools and/or specialized software are placed on systems to monitor data traffic or search for documents stored in electronic format.	• Real time monitoring may be difficult or may incur additional charges because USAID will no longer own the network. • Access to network logs, archived data, or other information may not be permitted. • Obtaining data for electronic discovery and litigation could be limited and delayed. • Inexpensive alternatives to search the network to obtain requested data may not exist. • Access to law enforcement information to build a case and take administrative or other action may be difficult to obtain or unavailable, which will result in insurmountable challenges for IG and Office of Security trying to investigate or discipline employees who are misusing or committing crimes using government resources. • Evidence requiring chain-of-custody may not be protected or difficult to maintain.

POTENTIAL RISK ASSOCIATED WITH CLOUD COMPUTING AT U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT		
	Description	**Risks**
5.	**Regulatory Compliance** is imposed by various statues and regulations, including the Privacy Act, the Freedom of Information Security Management Act (FISMA), the Federal Records Act, the Trade Secret Act and the Rehabilitation Act. Services obtained through cloud providers must be compatible with these requirements before committing to the provider's services.	• Non-compliance with federal regulations can be detrimental to USAID's operations and reputation. • Obtaining timely responses to USAID's or public request to access Freedom of Information Act information may not be permitted. • Protection of non-public information such as trade secrets, procurements, and pre-decisional policy information may not be adequate. • Physical security for responses to discovery and other informational disclosure requests may not be adequate. • Compliance with Section 508 of the U.S. Workforce Rehabilitation Act of 1973 that requires USAID's electronic and information technology to be accessible by people with disabilities may not be obtained. • Compliance with Privacy Act may not be obtained.
6.	**Portability and Interoperability** provides the agency with the ability to transfer and share data with other cloud providers and others	• Without identifying a backup cloud provider or backup plan and a means to allow data to be sharable between cloud providers, USAID could be at risk of not being able to process data and information.
7.	**Termination & Transition** ensures that agency data is properly protected, conveyed, and destroyed at the end of the cloud contract.	• Transfers to another cloud computing provider or if the provider goes out of business may be expensive. The transfer may require USAID to reformat its data and applications, and transfer them to a new provider, which could be a potentially complex and expensive process. • To bring the services provided by cloud computing vendor back in-house may not be easy or inexpensive. • Data may continue to reside on vendor's servers after the contract is terminated. • Timing of termination and transition could be disruptive to USAID's operations. • Ownership of data may not have been clearly defined and USAID may have to pay to obtain its data.

Source: CGIE IT Committee, Cloud Computing Contracting Concerns