Council of the
INSPECTORS GENERAL
on INTEGRITY and EFFICIENCY

The Council of the Inspectors General on Integrity and Efficiency's Cloud Computing Initiative

September 2014

Council of the Inspectors General on Integrity and Efficiency Cloud Computing Initiative

Executive Summary

Federal agencies have looked to leverage the benefits of cloud computing by incorporating cloud computing systems into their overall information technology (IT) environment. In response, the Council of the Inspectors General on Integrity and Efficiency's (CIGIE) IT Committee began a Government-wide initiative to evaluate participating agencies' efforts when adopting cloud computing technologies. As part of this consolidated cloud computing review, the 19 participating Offices of Inspector General (OIG) (see Appendix A) selected a sample of 77 commercial cloud contracts that Federal agencies issued as they transitioned to a cloud system.[1] These contracts have a value of approximately $1.6 billion (from a universe of 348 contracts totaling about $12 billion).[2] Each participating OIG reviewed its sampled contract(s) independently based on a standardized matrix of questions and verified its results through the respective OIG's internal quality control processes. Once the OIGs validated their results, they transmitted the results to the U.S. Department of Agriculture OIG for consolidation. Due to the variances in Federal contracts, not every element that was tested was applicable to every contract in the sample.

The majority of the participating OIGs have issued reports (See Appendix B), or plan to issue reports over the next few months, with agency specific recommendations.[3]

The testing that the OIGs conducted as part of the CIGIE initiative indicated that participating Federal agencies have not fully considered and implemented existing Federal guidance, the agencies' policies, and best practices when developing requirements for cloud computing contracts. The specificity of the requirements incorporated into the contracts used to procure cloud systems varied across the sample, with all 77 contracts lacking the detailed specifications recommended in Federal cloud computing guidelines and best practices documentation. Additionally, 59 cloud systems reviewed did not meet the requirement to become compliant with the Federal Risk Authorization and Management Program (FedRAMP) by June 5, 2014, even though the requirement was announced on December 8, 2011.[4] Finally, as the OIGs were validating their respective inventories, 9 of the 19 agencies found that they did not have an accurate and complete inventory of their cloud systems. These issues occurred in part because

[1] The total sample of commercial cloud contracts reviewed by the 19 OIGs was 77. However, the applicability of each question varied by contract. This resulted in a total response of less than 77 for some questions. For reporting purposes, the number reported is the number of 'No' responses per question for the total sample of 77 contracts.
[2] Due to the problems with validating the inventory for some participating agencies, the 348 contracts totaling $12 billion is based on the 348 known contracts identified by the participating agencies. Therefore, the actual dollar amount may be larger because the participating OIGs could not identify all of the cloud contracts. See Section 3 of this report.
[3] Some OIGs that are not issuing a report have discussed their findings with the agency and/or plan to include their findings in another report (i.e., their 2014 Federal Information Security Management Act report).
[4] One agency, which accounts for 4 of the 59 contracts, is not required to follow National Institute of Standards and Technology (NIST) or FedRAMP guidance. However, the agency has chosen to comply with some of the NIST standards and developed a cloud security policy requiring its cloud service providers to be FedRAMP-certified.

there is no single authoritative source that details the specifications agencies should consider when procuring cloud computing services and that requires Federal agencies to incorporate those specifications into cloud computing contracts. Additionally, although the Office of Management and Budget (OMB) established FedRAMP via a policy memorandum that also created the Joint Authorization Board (JAB) and the Program Management Office (PMO) to facilitate the FedRAMP authorization process, neither the JAB nor the PMO has the authority to enforce FedRAMP compliance within the individual agencies.[5] Since there is no discernable penalty for noncompliance and no singular governing body with the authority to enforce compliance, the agencies do not have an incentive to timely comply with FedRAMP requirements and therefore did not adequately plan in order to meet the June 5, 2014 deadline. Finally, many of the agencies that participated in the initiative had difficulty obtaining an accurate cloud system inventory due to a failure by agencies to report all cloud systems and a lack of consistency in applying cloud definitions.

Based on the findings in the report, none of the 19 participating agencies had adequate controls in place to manage its cloud service providers (CSP) and the data that reside within its cloud systems. This subjects Federal data to the risk of loss or exposure to unauthorized parties and could compromise both Federal program and personal data. Furthermore, because 42 contracts totaling approximately $317 million did not specify how a CSP's performance would be measured, reported, or monitored, the agencies are not able to ensure CSPs meet adequate service levels, which increases the risk that agencies could misspend or ineffectively use Government funds.

CIGIE's objective was to evaluate participating agencies' efforts when adopting cloud computing technologies and to review cloud service contracts for compliance with applicable standards.

CIGIE recommends that OMB:

- Establish standardized contract clauses that agencies must use when adopting cloud computing technologies;
- Determine how best to enforce FedRAMP compliance;
- Establish a process and reporting mechanism to ensure Federal agencies require CSPs to meet the FedRAMP authorization requirements in a timely manner; and
- Incorporate routine reviews of agency information system inventories into the continuous monitoring process.

[5] The JAB performs risk authorizations and grants the provisional FedRAMP authorization for the cloud system. Members of the JAB consist of the Chief Information Officers from the Department of Defense, Department of Homeland Security, and General Services Administration, and are supported by designated technical representatives from their respective member organizations.

Table of Contents

Background and Objectives

Background

The Council of the Inspectors General on Integrity and Efficiency (CIGIE) was statutorily established as an independent entity within the executive branch by the *Inspector General Reform Act of 2008*, Public Law 110-409. The mission of CIGIE is to:

- Address integrity, economy, and effectiveness issues that transcend individual government agencies; and

- Increase the professionalism and effectiveness of personnel by developing policies, standards, and approaches to aid in the establishment of a well-trained and highly skilled workforce in the Federal Inspector General (IG) community.

CIGIE Information Technology Committee

The CIGIE Information Technology (IT) Committee's mission is to facilitate effective IT audits, evaluations, and investigations by Offices of Inspector General (OIGs), and to provide a vehicle to express the IG community's perspective on Government-wide IT operations. Under its operating principles, this committee strives to promote participation by the IG community members in its activities; encourage communication and cooperation with colleagues in the IT field (including Federal Chief Information Officers and staff, and IT security professionals); and promote effective teamwork in addressing Government-wide initiatives, improving Federal Government IT activities, and safeguarding national IT assets and infrastructure.

The CIGIE IT Committee announced this initiative to perform a Government-wide review of agency cloud computing efforts to CIGIE members and 19 OIGs participated.[6] This review was modeled after an audit issued by the National Aeronautics and Space Administration (NASA) OIG on NASA's progress in adopting cloud computing technologies.[7] The U.S. Department of Agriculture (USDA) OIG agreed to coordinate this effort and prepare the consolidated report.

Cloud Computing Technology

The term "cloud computing" refers to information technology systems, software, and infrastructure that a service provider packages and sells to customers. The National Institute of Standards and Technology (NIST) describe the following five essential components of cloud systems, which are:[8]

[6] Federal Departments, Agencies, and other Federal entities were reviewed as part of the initiative. For our purposes in this report, all are referred to as Federal agencies throughout the report. See Appendix A for a list of participating OIGs.
[7] IG-13-021, *NASA's Progress in Adopting Cloud-Computing Technologies*, July 29, 2013 http://oig.nasa.gov/audits/reports/FY13/IG-13-021.pdf.
[8] NIST Special Publication (SP) 800-145, *The NIST Definition of Cloud Computing*, September 2011.

- On-demand self-service: The customer is able to provision computing capabilities with the service provider, as needed, without requiring human interaction.

- Broad network access: The customer accesses the capabilities (such as storage, servers, and databases) of the service provider through a network connection.

- Resource pooling: The customer shares vendor services with other customers.

- Rapid elasticity: The service provider's system allows the customer to rapidly expand or contract required computing resources.

- Measured service: The customer's payment for use of the cloud system is determined by a measured capability (such as seat licenses or storage used).

Cloud computing offers the potential for significant cost savings through more efficient delivery of computing resources, flexible payments that increase or decrease based on needed resources, and a decreased need to buy hardware or build data centers.

To accelerate the Federal Government's use of cloud computing strategies, the U.S. Chief Information Officer published the *Federal Cloud Computing Strategy,* requiring agencies to evaluate safe, secure cloud computing options before making any new IT investments.[9,10] Based on this "cloud first" policy, Federal agencies are to evaluate cloud services for new IT projects in an effort to realize the value of cloud computing through cost savings.

In addition to risks that resemble those of in-house information systems, cloud technologies have risks that are unique to a cloud system's deployment. For example, when using a cloud system, the customer relinquishes its ability to govern the system. Specifically, the client cedes control to the cloud service provider (CSP) on a number of issues that may affect security of the systems, such as incident management or patch management.[11,12] At the same time, service level agreements (SLAs) may not require CSPs to offer such services, thus leaving a gap in security defenses.[13,14]

As part of the consolidated cloud computing initiative, on behalf of CIGIE, USDA OIG received testing results from the 19 participating OIGs, resulting in a review of 77 contracts with a

[9] Kundra, V., *Federal Cloud Computing Strategy*, February 8, 2011.
[10] One of the agencies that participated in the cloud computing initiative is not required to follow OMB guidance.
[11] Incident management helps personnel to minimize loss or theft of information and disruption of services caused by incidents as well as to properly address legal issues that may arise during incidents.
[12] A patch is a small piece of software that is used to correct a problem with a software program or an operating system. Most major software companies will periodically release patches, usually downloadable from the internet, that correct very specific problems or security flaws in their software programs.
[13] European Network and Information Security Agency (ENISA) *Cloud Computing: Benefits, Risks and Recommendations for Information Security*, November 2009.
[14] An SLA is a document describing the level of service a customer expects from a provider. It lays out the metrics by which the customer will measure service, and the remedies or penalties, if any, should the supplier not achieve agreed-on levels.

reported value of approximately $1.6 billion (from a universe of 348 contracts with a value of approximately $12 billion). Although the total sample of contracts reviewed by the 19 OIGs was 77, the applicability of each question in the standardized matrix of questions varied by contract. This resulted in a total response of less than 77 for some questions. For reporting purposes, the number reported is the number of 'No' responses per question for the total sample of 77 contracts.

Objective

The objective of the CIGIE cloud computing initiative was to evaluate participating agencies' efforts when adopting cloud computing technologies and to review cloud service contracts for compliance with applicable standards.

Section 1: Cloud Contracting

Finding 1: Federal Agencies Need to Include More Detailed Cloud Contracting Specifications

Based on the results collected for the CIGIE cloud computing initiative, OIGs found that all 77 commercial cloud contracts reviewed did not include specifications for the agency and the CSP to adhere to, including detailed SLAs, data preservation responsibilities, roles and responsibilities, Federal regulation requirements, and audit and investigative access for OIGs.[15] Although the contracts tested did contain some of the elements, no one contract included all of the elements. This occurred in part because there is not a single, authoritative source that specifies the requirements agencies should consider when procuring cloud computing services and that requires Federal agencies to incorporate those requirements into cloud computing contracts. Additionally, in some instances, agencies had not implemented policies and procedures, or effective risk management processes, to ensure that all cloud contracts contained the provisions noted. As a result, the reviewed agencies have not implemented adequate controls in their contracts to monitor and manage their CSPs and the data that reside within the systems, subjecting Federal data to the risk of loss or exposure to unauthorized parties. Furthermore, because 42 contracts, totaling approximately $317 million, did not include detailed SLAs specifying how a provider's performance was to be measured, reported, or monitored, the agencies are not able to ensure that CSPs meet adequate service levels, which increases the risk that agencies could misspend or ineffectively use Government funds.

NIST recommends that if the terms of a default service agreement do not address all consumer needs, the consumer should discuss modifications to the SLA with the provider prior to use.[16] Regarding consumer needs, the Chief Information Officers (CIO) Council and the Chief Acquisition Officers (CAO) Council issued a cloud computing best practices report that provides specific guidance on how Federal agencies should effectively procure cloud services within existing regulations and laws.[17] For example, it suggests agencies establish terms of service (TOS) agreements that detail how end-users may use the services, the CSP's responsibilities, and how the CSP will deal with customer data. It also recommends that Federal agencies require CSPs to allow forensic investigations for both criminal and non-criminal purposes. In addition, the report recommends that the agency and CSP should have an SLA with clearly defined terms, definitions, and penalties for failure to meet SLA performance measures.

Specific details of our testing are as follows.

[15] Data preservation responsibilities address how long the CSP must maintain the agency's data, whether the agency or CSP retains the data ownership rights, and how the CSP should sanitize the data throughout the system lifecycle.
[16] The default SLAs of public clouds specify limited promises that providers make to consumers, limit the remedies available to consumers, and outline consumer obligations in obtaining such remedies. NIST SP 800-146, *Cloud Computing Synopsis and Recommendations*, May 2012.
[17] The CIO Council and CAO Council guidance, *Creating Effective Cloud Computing Contracts for the Federal Government Best Practices for Acquiring IT as a Service*, February 24, 2012.

Service Level Agreement

OIGs found that 64 cloud contracts reviewed lacked detailed SLAs, which define the expected level of service the CSP will deliver and the service credit available to the consumer if the CSP fails to deliver the service at the specified level.[18] For example, OIGs found that 42 contracts did not specify how a provider's uptime percentage performance (the level of system availability that the CSP must provide to the agency for a specific period of time) was to be measured, reported, or monitored. Specifically, of the 42 contracts, OIGs found:

- 15 contracts reviewed did not specify the required uptime percentages for the CSP.

- 24 contracts did not describe how the uptime percentage was calculated. This calculation is critical so that the agency can verify the CSP is meeting the stated uptime percentages.

- 27 contracts did not detail remedies the CSP would pay to the agency if the CSP did not meet uptime requirements. NIST SP 800-146 states that if a CSP fails to provide the stated availability, the CSP should compensate consumers in good faith with a service credit for future use of cloud services.

- 23 contracts did not assign someone from the agency to monitor the actual uptime, compare it to the uptime percentage specified in the contract, and pursue service credits, when applicable. NIST SP 800-146 states that the consumer is generally responsible for obtaining a service credit and the consumer must provide timely information about the nature and the time length of the outage.

If an agency does not monitor and verify the uptime percentage, the agency cannot be assured that it will receive a service credit if the CSP does not meet its uptime percentages.

Data Preservation

OIGs found that 34 cloud contracts did not include data preservation requirements. Data preservation responsibilities should address how long the CSP must maintain the agency's data, whether the agency or CSP retains the data ownership rights, and how the CSP should sanitize data throughout the system lifecycle.[19]

Non-Disclosure Agreements (NDAs)

OIGs found that 33 CSPs did not sign an NDA with the agency to protect non-public information that is procurement-sensitive, or affects pre-decisional policy, physical security, or other information deemed important to protect.

[18] NIST SP 800-144, *Guidelines on Security and Privacy in Public Cloud Computing*, December 2011.
[19] NIST SP 800-144, *Guidelines on Security and Privacy in Public Cloud Computing*, December 2011.

Since CSP personnel have access to, and control of the Federal data residing in the cloud system, NDAs are a critical control to ensure CSPs protect the information being stored in the cloud.[20]

In addition, the 39 contracts that included NDAs were reviewed and OIGs found that 27 did not establish rules of behavior specifically within the NDA for the CSP, nor did they establish a method within the NDA for the agency to monitor end-user activities in the cloud environment.[21] Defining a method for the agency to monitor end-user activities provides the agency with a process to verify adherence to the NDA.

Roles and Responsibilities

OIGs found that 22 contracts did not contain TOS specifications. TOS requirements generally include how end-users may use the services, the responsibilities of the CSP, and how the CSP will handle customer data. To effectively manage cloud services, the Federal agency and the CSP must clearly define their roles and responsibilities. NIST states that an agency should understand both its responsibilities and those of the CSP before using a cloud service. Accordingly, the CSPs and the agencies must agree to all terms to ensure that both parties fully understand their duties when providing and using a cloud service.

Federal IT Regulatory Requirements

OIGs found that 44 contracts did not completely address applicable Federal rules and regulations. In addition to contract roles and responsibilities, agencies that use cloud computing contracts are subject to unique policy and regulatory requirements. Federal agencies must ensure that any selected cloud computing solution is configured, deployed, and managed to meet the security, privacy, and other requirements of the organization.[22] Furthermore, NIST states that the Federal Information Security Management Act of 2002 (FISMA) and the associated NIST standards and special publications (e.g., FIPS 199, FIPS 200, SP 800-53) are applicable to cloud systems.[23]

Access to CSPs for Audit and Investigative Purposes

From the sampled contracts that were reviewed for the presence of specifications for audit and investigative access in cloud contracts, the OIGs found the following:

[20] The CIO Council and CAO Council guidance, *Creating Effective Cloud Computing Contracts for the Federal Government Best Practices for Acquiring IT as a Service*, February 24, 2012.
[21] The rules of behavior, which are required in OMB Circular A-130, Appendix III, and are a security control contained in NIST SP 800-53, should clearly delineate the responsibilities and expected behavior of all individuals with access to the system. NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.
[22] NIST SP 800-144, *Guidelines on Security and Privacy in Public Cloud Computing*, December 2011.
[23] One of the agencies that participated in the cloud computing initiative is not required to follow NIST guidance, but considers the guidance to be a best practice.

- 61 contracts reviewed did not include language to allow agencies to conduct forensic investigations for both criminal and non-criminal purposes without interference from the CSP.

- 65 contracts did not detail procedures for electronic discovery when conducting a criminal investigation.

- 54 contracts did not include language to allow the OIG full and unrestricted access to the contractor's (and subcontractor's) facilities, installations, operations, documentation, databases, and personnel used in performance of the contract in order to conduct audits, inspections, investigations, or other reviews.

OIG offices of audit and investigations must have access to CSP and subcontractor personnel, facilities, and Federal agency information to perform their statutory oversight roles. The CIO Council and CAO Council cloud computing best practices report states that Federal agencies should require CSPs to allow forensic investigations for both criminal and non-criminal purposes, and these investigations should be able to be conducted without affecting data integrity and without interference from the CSP.[24]

Without proper access to the CSP and the services being provided, OIGs cannot verify that appropriate security controls are in place to reduce risk to a level acceptable to the agency. Additionally, limiting OIG access to CSP facilities and data could compromise and interfere with audits and criminal investigations.

The nature of cloud computing requires customers to cede control to the CSP on a number of issues that may affect security, such as incident management or patch management. At the same time, service agreements may not offer or include a commitment from the CSP to provide such services, thus leaving a gap in security.[25] Without detailed contract specifications that include SLAs, data preservation responsibilities, roles and responsibilities, regulation requirements, and audit and investigative access, the Federal Government's data stored within the cloud environment could be at risk, which affects all Federal programs, personnel, and citizen data in the cloud environment. Additionally, without the ability to determine how the CSPs' performance is measured, reported, or monitored, the Government does not have the ability to ensure that CSPs are meeting required service levels, which increases the risk that agencies could misspend or ineffectively use Government funds.

CIGIE concluded that Federal agencies must take steps to ensure that cloud computing arrangements are meeting the needs of the Government. OMB should develop guidance specifying the clauses agencies must incorporate into cloud computing contracts.

[24] Recognizing this issue, the CIGIE IT Committee drafted clauses that would ensure OIG audit and investigative access and proposed including the clauses in the Federal Acquisition Regulation (FAR) to the FAR Council in January 2012.
[25] European Network and Information Security Agency (ENISA), *Cloud Computing: Benefits, Risks, and Recommendations for Information Security*, November 2009.

Recommendation 1

OMB needs to develop guidance defining a minimum set of requirements that Federal agencies must incorporate into a cloud contract when they adopt cloud computing technologies.

Section 2: FedRAMP Compliance

Finding 2: Federal Agencies Must Meet FedRAMP Requirements

OMB issued a policy memorandum on December 8, 2011 requiring cloud systems utilized by executive departments and agencies to be FedRAMP compliant by June 5, 2014. OIGs determined that 59 reviewed systems were not compliant with FedRAMP by the required deadline of June 5, 2014. FedRAMP establishes a risk-based approach for adopting and using cloud services and includes standardized security requirements.[26] Sixteen of the nineteen agencies participating in this review had contracts that did not meet this deadline. Ultimately, this occurred because the agencies did not adequately plan in order to meet the June 5th deadline and the FedRAMP PMO does not have the authority to enforce FedRAMP compliance at the agency level. Additionally, agencies reported that their contractors were noncompliant because the contractors did not believe they were required to be FedRAMP compliant. Compounding the problem, the OIGs found that for 30 of the 59 noncompliant systems, the agencies did not establish a comprehensive inventory of all cloud services.[27] FedRAMP states that establishing an inventory of all cloud services within an agency is a critical step on the path to FedRAMP compliance. Once the agency establishes its inventory, it needs to work with CSPs to update contractual requirements and determine the path each cloud system will take to become FedRAMP compliant. FedRAMP's purpose is to ensure that cloud-based services have an adequate information security program that addresses the specific characteristics of cloud computing and provides the level of security necessary to protect government information. The failure of the cloud system to address and meet FedRAMP security controls increases the risk that Federal program data may be compromised, intercepted, or lost, which could expose the data to unauthorized parties.

FedRAMP was announced on December 8, 2011, via an OMB policy memorandum, that addressed the security authorization process for cloud computing services.[28] In the memorandum, OMB requires each executive department or agency to use FedRAMP when conducting risk assessments and security authorizations, and granting an authority to operate for the use of cloud services. FedRAMP's goal is to provide a cost-effective, risk-based approach for adopting and using cloud services. It includes:

- Standardized security requirements for the authorization and ongoing cybersecurity of cloud services for selected information system impact levels;[29]

[26] One agency, accounting for 4 of the 59 contracts, is not required to follow FedRAMP guidance. However, the agency has chosen to comply with these requirements and developed a cloud security policy requiring its cloud service providers to be FedRAMP-certified.
[27] Nine of the nineteen agencies that participated in the CIGIE cloud initiative noted inventory issues.
[28] OMB Memorandum for Chief Information Officers, *Security Authorization of Information Systems in Cloud Computing Environments* (December 8, 2011).
[29] The system's security category is determined in accordance with Federal Information Processing Standard 199. After the category is determined, the contractor should apply the appropriate set of baseline controls as required in the FedRAMP Cloud Computing Security Requirements Baseline document to ensure compliance with security standards. The FedRAMP baseline controls were originally based on NIST SP 800-53, Revision 3. An updated security control baseline was released on June 6, 2014, based on Revision 4.

- An assessment program capable of producing consistent independent, third-party assessments of security controls implemented by CSPs;

- Authorization packages of cloud services reviewed by a JAB consisting of security experts from the Department of Homeland Security, Department of Defense, and the General Services Administration;[30]

- Standardized contract language to help executive departments and agencies integrate FedRAMP requirements and best practices into acquisitions of cloud systems; and

- A repository of authorization packages for cloud services that can be leveraged Government-wide.

Due to the unique risks presented by cloud computing environments, FedRAMP incorporated controls from NIST SP 800-53 into its baseline security control framework for use with cloud systems. According to OMB, all cloud services currently implemented were required to comply with FedRAMP by June 5, 2014.

CIGIE concluded that OMB needs to strengthen Federal agencies' compliance with FedRAMP's requirements.

Recommendation 2

OMB needs to determine how best to enforce FedRAMP compliance.

Recommendation 3

OMB needs to establish a process and reporting mechanism to ensure Federal agencies require CSPs to meet the FedRAMP authorization requirements in a timely manner.

[30] Authorization packages contain the body of evidence needed by authorizing officials to make risk-based decisions regarding the information systems providing cloud services. This includes, at a minimum, the security plan, security assessment report, plan of action and milestones, and a continuous monitoring plan.

Section 3: Cloud Inventory Management

Finding 3: Federal Agencies Must Develop Accurate Cloud System Inventories

During the course of work performed by the OIGs for the CIGIE cloud computing initiative, they determined that 9 of 19 agencies did not have an accurate and complete inventory of their cloud systems. This occurred in many instances because the inventory process at select agencies relied on manual reporting of the systems to a centralized office, such as the CIO's office; the agency officials were not consistently applying the NIST definition of cloud computing; or a combination of both. Without accurate and complete inventories, the agencies involved do not know the extent to which their data reside outside their own information system boundaries and are subject to the inherent risks of cloud systems. These risks include isolation failure, interception of data in transit, and insecure or ineffective deletion of data.[31] These risks could expose agency data to unauthorized parties and potentially compromise the objectives of the agencies' programs.

OMB requires Federal agencies to follow NIST guidance.[32] According to NIST, Federal agencies need to develop and document an inventory of information system components that: (1) accurately reflects the current information system, (2) includes all components within the authorization boundary of the information system, and (3) includes the granularity deemed necessary for tracking and reporting.[33]

In addition, the Council on Cybersecurity designated an inventory of hardware and an inventory of software as the top two critical security controls for building a secure network.[34] The critical controls are a recommended set of actions for cyber defense that provide specific and actionable ways to mitigate the most pervasive attacks. Attackers are continuously scanning the address space of target organizations, waiting for new and unprotected systems to be attached to a network. Therefore, it is critical to maintain an asset inventory of all systems connected to the network, including the network devices themselves, and to include every system that has an Internet protocol address on the network. Without an accurate and complete cloud system inventory, agencies cannot ensure the appropriate controls are in place to protect the systems and their data.

[31] Isolation failure is the failure of the mechanisms that separate the data of different clients on the same cloud, thus exposing sensitive data to unauthorized users. Interception of data in transit occurs when an unauthorized party uses sniffing or man-in-the-middle attacks to intercept data being sent to or from the cloud. Insecure or ineffective deletion of data occurs when data are not truly erased from the cloud at the end of a cloud service contract.
[32] OMB M-14-04, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,* November 18, 2013.
[33] NIST SP 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* April 2013.
[34] The Council on Cybersecurity is a consortium of U.S. and international agencies and experts from private industry and around the globe. They provided recommendations for what ultimately became the critical security controls. In 2013, the stewardship and sustainment of the controls was transferred to the Council on Cybersecurity, an independent, global non-profit entity committed to a secure and open Internet.

CIGIE views the consistent application of a cloud computing definition, in accordance with NIST guidance, as a critical element for establishing a complete and accurate inventory of cloud systems. CIGIE concluded that all Federal agencies need to ensure that they have an accurate and complete inventory of their cloud-based systems.

Recommendation 4

OMB needs to incorporate routine reviews of agency information system inventories into the continuous monitoring process.

Scope and Methodology

This report is a compilation of the results of a Government-wide review initiated by the CIGIE IT Committee and conducted by Federal OIGs. The objective was to conduct a Government-wide review of Federal agencies' cloud computing efforts using a standard methodology based on an audit program developed by NASA OIG. The NASA OIG had used the program in an earlier audit of cloud computing efforts at NASA. CIGIE invited all Federal OIGs to take part in this consolidated effort, and 19 OIGs participated (see Appendix A). USDA OIG agreed to coordinate this effort on behalf of CIGIE.

The report was prepared to highlight crosscutting issues and lessons learned from the Government-wide review. As a result, CIGIE provided recommendations for OMB's consideration. In compiling the results contained in this report, USDA OIG did not conduct or perform any additional audit work pertaining to the results received.

Based on the information obtained by the 19 participating OIGs, the universe contained 348 commercial cloud contracts with a value of about $12 billion. Each participating OIG used its own sampling methodology to select a sample of cloud IT services and service providers that had active contracts in fiscal year (FY) 2014.[35] For example, some agencies judgmentally selected cloud service providers based on contract value, system risk, or a combination of the two. The total sample of contracts reviewed by the 19 OIGs was 77; however, the applicability of each question varied by contract. This resulted in a total response of less than 77 for some questions. For reporting purposes, the number reported is the number of 'No' responses per question for the total sample of 77 contracts.

To answer the objectives of this coordinated review, 18 of the 19 participating OIGs were provided a standardized matrix of questions to ensure each of the participating OIGs had a consistent foundation for developing their testing methodologies. For the remaining OIG, NASA, USDA OIG used its final audit report to incorporate applicable testing results—Appendix B contains a link to NASA's report. Each participating OIG conducted its review independently and verified its results through its internal quality control process. Once an OIG validated its results, it transmitted those results to USDA OIG for consolidation. USDA OIG relied on the participating OIGs internal quality control review process and therefore did not do any audit work to validate the results received.

Participating OIGs used a combination of methodologies to obtain each agency's testing results, including inspections, evaluations, and audits in compliance with generally accepted government auditing standards (GAGAS) procedures. Therefore, the consolidated report is not a GAGAS compliant performance audit. To accomplish the initiative's objectives, each participating OIG interviewed applicable personnel and reviewed supporting documentation, as necessary, for a sample of cloud systems under contract in FY 2014 to determine compliance with applicable Federal and agency standards.

[35] The NASA OIG report was issued July 29, 2013 and the results from this report were included in this consolidated report. The scope of that report included cloud contracts that were in effect while audit fieldwork was conducted from June 2012 to June 2013.

For this review, each OIG obtained an inventory of its agency's cloud systems. Some OIGs solicited the information from their agencies through a survey, others obtained an inventory list from their Office of the Chief Information Officer, and some used both methods. Due to inventory issues noted, agencies could not verify the completeness or accuracy of their cloud systems inventory; therefore, USDA OIG cannot be certain that all cloud systems were identified for inclusion in the agencies' universe. Additionally, due to the large number of cloud service contracts reported by the participating OIGs, USDA OIG could not verify the accuracy of the dollar values associated with the inventory provided.

Personnel from participating OIGs conducted fieldwork between January and August 2014, at applicable agency locations throughout the United States.[36]

[36] The NASA audit report was issued July 29, 2013, based on field work conducted from June 2012 – June 2013.

Abbreviations

CAO ..... Chief Acquisition Officer
CIGIE ..... Council of the Inspectors General on Integrity and Efficiency
CIO ..... Chief Information Officer
CSP ..... cloud service provider
ENISA ..... European Network and Information Security Agency
FAR ..... Federal Acquisition Regulation
FedRAMP ..... Federal Risk and Authorization Management Program
FISMA ..... Federal Information Security Management Act
FY ..... fiscal year
GAGAS ..... generally accepted government auditing standards
IG ..... Inspector General
IT ..... information technology
JAB ..... Joint Authorization Board
NASA ..... National Aeronautics and Space Administration
NDA ..... non-disclosure agreement
NIST ..... National Institute of Standards and Technology
OIG ..... Office of Inspector General
OMB ..... Office of Management and Budget
PMO ..... Program Management Office
SLA ..... service level agreement
SP ..... special publication
TOS ..... terms of service agreements
USDA ..... U. S. Department of Agriculture

Appendix A: List of Participating Offices of Inspector General

The OIGs for the following agencies participated in the CIGIE Cloud Computing initiative, and this report reflects their results.

1. Department of Agriculture (USDA)
2. Department of Commerce (DOC)
3. Department of Education (Ed)
4. Department of Energy (DOE)
5. Department of the Interior (DOI)
6. Department of Justice (DOJ)
7. Department of Labor (DOL)
8. Department of Transportation (DOT)
9. Environmental Protection Agency (EPA)
10. General Services Administration (GSA)
11. National Aeronautics and Space Administration (NASA)
12. National Endowment for the Humanities (NEH)
13. National Labor Relations Board (NLRB)
14. Board of Governors of the Federal Reserve System and the Consumer Financial Protection Bureau (CFPB)
15. Office of Personnel Management (OPM)
16. Pension Benefit Guaranty Corporation (PBGC)
17. Social Security Administration (SSA)
18. United States Agency for International Development (USAID)
19. United States Postal Service (USPS)

Appendix B: Individual Reports Issued as Part of the CIGIE Cloud Computing Initiative

Some participating OIGs have completed and published agency-level reports as part of the work performed in conjunction with the CIGIE Cloud Computing initiative. Some OIGs have work in process and will be issuing agency level reports in the future. If an OIG has released a report, the following table includes a link to its released report.

Agency	Report Link
DOE	http://energy.gov/node/962096
EPA	http://www.epa.gov/oig/reports/2014/20140724-14-P-0323.pdf
NASA	http://oig.nasa.gov/audits/reports/FY13/IG-13-021.pdf
NLRB	https://www.nlrb.gov/sites/default/files/attachments/basic-page/node-1700/OIG-AMR-74-14-03%20-%20%20Cloud%20Computing.pdf
OPM	http://www.opm.gov/our-inspector-general/reports/2014/status-of-cloud-computing-environments-within-opm-4a-ci-00-14-028.pdf
USDA	http://www.usda.gov/oig/webdocs/50501-0005-12.pdf
USPS	https://www.uspsoig.gov/sites/default/files/document-library-files/2014/it-ar-14-009.pdf