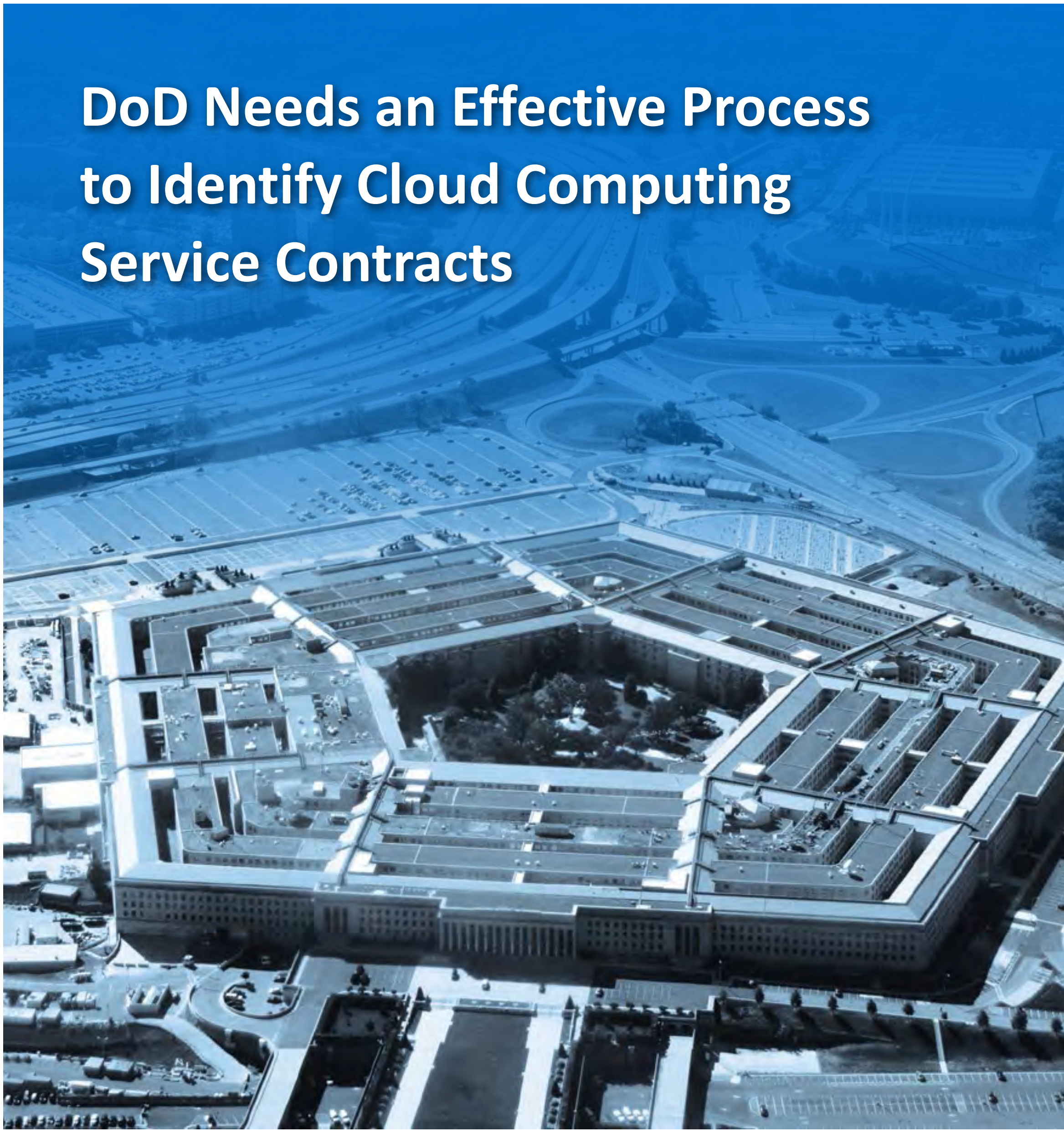
Report No. DODIG-2016-038

INSPECTOR GENERAL

U.S. Department of Defense

DECEMBER 28, 2015

DoD Needs an Effective Process to Identify Cloud Computing Service Contracts



INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

Mission

Our mission is to provide independent, relevant, and timely oversight of the Department of Defense that supports the warfighter; promotes accountability, integrity, and efficiency; advises the Secretary of Defense and Congress; and informs the public.

Vision

Our vision is to be a model oversight organization in the Federal Government by leading change, speaking truth, and promoting excellence—a diverse organization, working together as one professional team, recognized as leaders in our field.

Fraud, Waste & Abuse
HOTLINE
Department of Defense
dodig.mil/hotline | 800.424.9098

For more information about whistleblower protection, please see the inside back cover.

Results in Brief

DoD Needs an Effective Process to Identify Cloud Computing Service Contracts

December 28, 2015

Objective

Our objective was to determine whether selected DoD Components performed a cost-benefit analysis before acquiring cloud computing services. In addition, we were to identify whether those DoD Components achieved actual savings as a result of adopting cloud services.

Due to the limited number of cloud computing service contracts identified, we could not provide a sufficient answer to our announced objective. However, we addressed the need for a standardized cloud computing definition and an integrated repository for cloud computing service contract information to help determine whether DoD is effectively using cloud computing services.

Finding

DoD did not maintain a comprehensive list of cloud computing service contracts. This occurred because the DoD Chief Information Officer (CIO) did not establish a standard, Department-wide definition for cloud computing and did not develop an integrated repository that could provide detailed information to identify cloud computing service contracts.

As a result, DoD cannot measure the effectiveness of the DoD cloud computing initiative. Specifically, DoD cannot determine whether it achieves actual cost savings or benefits from adopting cloud computing services. In addition, without knowing what data DoD Components place on the cloud, DoD may not effectively identify and monitor cloud computing security risks.

Visit us at www.dodig.mil

Recommendations

We recommend that the DoD CIO:

- issue guidance to either establish a standard, Department-wide cloud computing definition or clarify the National Institute of Standards and Technology definition to consistently identify DoD Component cloud computing service contracts; and
- establish an integrated repository that provides detailed information to identify DoD cloud computing service contracts after Recommendation 1.a of this report is completed.

Management Comments and Our Response

The Principal Deputy DoD CIO, responding for the DoD CIO, neither agreed nor disagreed with the report recommendations, but provided actions taken by the DoD CIO to address the recommendations. However, the responses provided did not address the specifics of Recommendation 1.a and partially addressed Recommendation 1.b. Therefore, we request that DoD CIO provide additional comments in response to this report by January 27, 2016. Please see the Recommendations Table on the back of this page.

Recommendations Table

Management	Recommendations Requiring Comment	No Additional Comments Required
DoD Chief Information Officer	1.a, 1.b	

Please provide Management Comments by January 27, 2016.

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

December 28, 2015

MEMORANDUM FOR DOD CHIEF INFORMATION OFFICER

SUBJECT: DoD Needs an Effective Process to Identify Cloud Computing
Service Contracts (Report No. DODIG-2016-038)

We are providing this report for review and comment. DoD did not maintain a comprehensive list of cloud computing service contracts. As a result, DoD cannot determine whether it achieves actual savings or benefits from adopting cloud computing services and may not effectively identify and monitor cloud computing security risks. We conducted this audit in accordance with generally accepted government auditing standards.

We considered management comments on a draft of this report when preparing the final report. DoD Instruction 7650.03 requires that recommendations be resolved promptly. Comments from the DoD Chief Information Officer did not address recommendation 1.a, and partially addressed Recommendation 1.b. Therefore, we request that the DoD Chief Information Officer provide additional comments on Recommendations by January 27, 2016.

Please send a PDF file containing your comments to audrco@dodig.mil. Copies of your comments must have the actual signature of the authorizing official for your organization. We cannot accept the /Signed/ symbol in place of the actual signature. If you arrange to send classified comments electronically, you must send them over the SECRET Internet Protocol Router Network (SIPRNET).

We appreciate the courtesies extended to the staff. Please direct questions to me at (703) 699-7331 (DSN 499-7331).

Carol N. Gorman

Carol N. Gorman
Assistant Inspector General
Readiness and Cyber Operations

Contents

Introduction

Finding. DoD Did Not Maintain a List Of Cloud Computing Service Contracts

Appendix

Management Comments

Introduction

Objective

Our objective was to determine whether selected DoD Components performed a cost-benefit analysis before acquiring cloud computing services. In addition, we were to identify whether those DoD Components achieved actual savings as a result of adopting cloud services.

Due to the limited number of cloud computing service contracts identified, we could not provide a sufficient answer to our announced objective. However, we addressed the need for a standardized cloud computing definition and an integrated repository for cloud computing service contract information to help determine whether DoD is effectively using cloud computing services. See Appendix for discussion of our scope and methodology and prior audit coverage.

Background

Cloud computing is a subscription-based service that provides network-based storage space and computer resources. It allows users to store and access data and programs over the internet rather than a computer hard drive. It also allows users to access information from anywhere at any time, effectively removing the need for the user to be in the same physical location as the hardware that stores the data.

There are three types of cloud service models:

- Software as a Service
- Platform as a Service
- Infrastructure as a Service

The three types differ in the amount of control that the user has over the information, and, conversely, how much the user can expect the provider to do for them. Users should understand the security measures that their cloud provider has in place to secure data placed on the cloud, which vary from provider to provider and among the various types of clouds.

In December 2010, the U.S. Chief Information Officer (CIO) released the "25 Point Implementation Plan to Reform Federal Information Technology Management." The plan directs the Federal Government to shift to a "Cloud First" policy that requires agencies to default to cloud-based solutions when evaluating options for new information technology (IT) deployments if a secure, reliable, cost-effective cloud-option exists.

In February 2011, the U.S. CIO released the "Federal Cloud Computing Strategy" to provide additional information on adoption of cloud computing. According to the Federal Strategy, cloud computing could assist agencies to consolidate facilities and reduce IT service costs while increasing IT service responsiveness.

In July 2012, the DoD CIO released the "Department of Defense Cloud Computing Strategy" that emphasized the DoD commitment to realize the value of cloud computing and provide a secure enterprise cloud environment, in alignment with Federal and DoD-wide IT efficiency initiatives. The goal of the strategy was to increase the Department's secure information sharing and collaboration, enhance mission effectiveness, and decrease costs using cloud computing services.

Review of Internal Controls

DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013, requires DoD organizations to establish a program to review, assess, and report on the effectiveness of their internal controls. We identified internal control weaknesses in DoD's management of the cloud computing initiative. Specifically, the DoD CIO did not establish a standard, Department-wide definition for cloud computing. In addition, DoD CIO did not develop an integrated repository that could provide detailed information to identify cloud computing service contracts. We will provide a copy of the report to the senior official responsible for internal controls in the Office of the DoD CIO.

Finding

DoD Did Not Maintain a List Of Cloud Computing Service Contracts

DoD did not maintain a comprehensive list of cloud computing service contracts. This occurred because the DoD CIO did not establish a standard, Department-wide definition for cloud computing and did not develop an integrated repository that could provide detailed information to identify cloud computing service contracts. As a result, DoD cannot measure the effectiveness of the DoD cloud computing initiative. Specifically, DoD cannot determine whether it achieves actual cost savings or benefits from adopting cloud computing services. In addition, without knowing what data DoD Components place on the cloud, DoD may not effectively identify and monitor cloud computing security risks.

DoD Used Various Sources to Compile a List of Cloud Computing Service Contracts

DoD CIO representatives did not maintain a list of cloud computing service contracts and, therefore, could not provide a reliable list of cloud computing service contracts issued from FY 2011 through FY 2014. Instead, the representatives said they used various sources to compile a list. However, cloud computing service contract information provided by the Military Department representatives did not always match what the DoD CIO representatives provided.

DoD CIO representatives acknowledged that DoD reporting systems were not configured to collect and provide a reliable inventory. Therefore, when we requested a list of DoD Components that acquired cloud computing service contracts from FY 2011 through FY 2014, DoD CIO representatives said they had to compile a list based on various sources such as informal data calls and coordination with IT working groups. However, they recognized the list may not be complete. The list DoD CIO representatives provided contained information for the Army, Navy, Air Force and two Defense agencies. Based on the results of the list DoD CIO representatives provided, we focused our review on the Military Departments.

...DoD CIO representatives said they had to compile a list based on various sources... However, they recognized the list may not be complete.

However, information we obtained from DoD CIO representatives in response to our request covering FY 2011 through FY 2014 and information we obtained from Military Department representatives for that same period did not always match. For example, the DoD CIO list contained three Army indefinite-delivery indefinite-quantity (IDIQ) contracts for cloud computing services while the Army Contracting Command provided six additional IDIQ contracts for cloud computing services. Although the IDIQ contracts were issued by Army Contracting Command, they are available for all DoD Components to use; however components must issue a task order against the contract to obtain the cloud computing services offered. The Army Contracting Command identified only two task orders issued on the IDIQs.

Further, the DoD CIO list identified two potential Navy cloud computing service contracts but did not contain corresponding contract numbers. According to Navy CIO representatives, the Navy did not have an operational cloud computing service contract. Specifically, Navy CIO representatives stated that "all Navy commercial clouds are pilot programs," which the Navy used to identify and resolve numerous lessons and challenges with a proposed cloud solution. Finally, the DoD CIO list identified two potential Air Force cloud computing service contracts. However, Air Force CIO representatives' verified only one operational Air Force cloud computing service contract issued from FY 2011 through FY 2014. See the Table for a summary of the inconsistencies.

Table. Cloud Computing Service Contracts

Military Department	DoD CIO Identified	Military Department Identified
Army	3 IDIQ contracts	9 IDIQ contracts
Navy	2 potential contracts	0 contracts
Air Force	2 potential contracts	1 contract

The Defense Information Systems Agency (DISA) served as the DoD cloud service broker from 2012 through 2014[1] and maintained a list of the DoD Components that inquired about cloud computing services. We obtained DISA's cloud service request list to determine the Military Departments that may have acquired cloud computing services based on those inquiries. We did not identify any additional cloud computing service contracts using DISA's list.

[1] DoD CIO Memorandum, "Designation of the Defense Information Systems Agency as the Department of Defense Enterprise Cloud Service Broker," June 26, 2012, required DoD Components to acquire cloud computing services using the broker or obtain a waiver.

DoD Lacked a Standard Cloud Definition and Integrated Repository

The DoD CIO did not establish a standard, Department-wide definition for cloud computing but did refer components to the National Institute of Standards and Technology (NIST) cloud computing definition. In addition, the DoD CIO did not have an integrated repository that provided detailed information to allow the DoD CIO to obtain information on cloud computing service contracts.

DoD Did Not Establish a Standard Definition for Cloud Computing

The DoD CIO Cloud Computing Strategy refers DoD Components to the NIST definition for cloud computing. NIST[2] defines cloud computing as:

> A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

The model has five essential characteristics:

- **On-demand self-service.** Requires no human interaction with service providers.
- **Broad network access.** Capabilities available over the network and accessed through mechanisms such as mobile phones, tablets, and laptops.
- **Resource pooling.** Provider's computing resources are pooled to serve multiple consumers with different physical and virtual resources assigned based on consumer demand.
- **Rapid elasticity.** Capabilities available for provisioning often appear unlimited to the consumer and can be appropriated in any quantity at any time.
- **Measured service.** Cloud systems automatically control and optimize resource use which can be monitored, controlled, and reported, providing transparency for both the provider and consumer.

[2] U.S. Department of Commerce NIST Special Publication 800-145 "The NIST Definition of Cloud Computing," September 2011.

Although DoD Components stated they used the NIST definition, the definition was interpreted differently by the Components.

Although DoD Components stated they used the NIST definition, the definition was interpreted differently by the Components. For example, DoD CIO representatives stated that an IT service did not have to possess all five essential characteristics of the NIST cloud definition to be considered a cloud computing service. Air Force CIO representatives stated they considered all five essential characteristics needed to classify an IT service as a cloud computing service. Navy CIO representatives stated there was a lack of clarity to determine whether a service had to meet all NIST characteristics. They further stated that two characteristics, "self-service" and "broad network access," were less well defined, which made it difficult to agree if a service provided met the cloud definition.

Finally, according to DISA representatives, cloud computing services offered by DISA did not always meet all of the cloud computing attributes cited by NIST and as an example, DISA cited Defense Enterprise Email. Specifically, DISA representatives stated:

> A Defense Enterprise Email customer pays for a certain amount of email storage per user but the storage does not automatically scale up to the next increment in response to excess demand. However, Defense Enterprise Email is a service that is always available and can be accessed from anywhere.

DISA representatives concluded that the designation of an IT service as cloud depends on individual perspective.

Without a clear, standard, Department-wide definition for cloud computing, DoD Components do not consistently identify their use of cloud computing services. Although DoD CIO representatives said they used the NIST definition for cloud computing, DoD's lack of clarity of the definition allowed DoD Components to interpret it differently. DoD CIO should establish a standard, Department-wide definition of cloud computing or clarify the NIST definition, including the five characteristics, to help ensure all DoD Components consistently identify future cloud computing efforts.

DoD Lacked a Repository for Cloud Computing Service Contract Information

The DoD CIO did not have an integrated repository that would allow them to obtain cloud computing service contract information. DoD CIO representatives said they used the following four IT reporting systems to gather information on DoD cloud computing.

- DoD IT Portfolio Repository,
- Select and Native Programming Data Input System for IT,
- DoD IT Investment Portal, and
- System and Network Approval Process.

According to DoD CIO representatives, DoD reporting systems need to be improved before they could provide "a good inventory of cloud computing activity." Specifically, DoD CIO representatives stated that DoD reporting systems were not integrated and did not provide the level of detail on DoD cloud computing desired by the DoD CIO. According to the representatives, they were examining potential reporting system improvements, but those improvements were not expected before FY 2016. For example, the DoD CIO representatives stated the DoD CIO was trying to determine how to better link reporting systems.

...DoD CIO representatives stated that DoD reporting systems were not integrated and did not provide the level of detail on DoD cloud computing desired by the DoD CIO.

In addition to examining improvements to existing IT reporting systems, the Acting DoD CIO issued guidance to improve the process of acquiring cloud computing services and maintain a level of oversight. On December 15, 2014, the Acting DoD CIO issued updated guidance[3] that required DoD Components to use a Business Case Analysis (BCA) template[4] to analyze each use of cloud computing services and provide the results to the DoD CIO. DoD Components employ the Enterprise IT BCA template to analyze cloud service investments, and determine which cloud service provider to use for a specific set of information or mission. According to DoD CIO representatives, they would retain each BCA for further review of completeness, general accuracy, logical framework, compliance with the DoD cloud strategy, and actual versus projected results.

[3] Acting DoD CIO Memorandum, "Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services," December 15, 2014.

[4] For the Air Force contract we identified, although the Air Force did not conduct a BCA prior to issuing the contract, they prepared a BCA in January 2015 in accordance with the December guidance.

Retaining the BCAs would provide DoD CIO visibility into DoD Component use of cloud computing services. However, preparing a BCA alone does not mean that a component will ultimately issue a contract to acquire that cloud service, only that the component has considered options to acquire it. Therefore, DoD CIO needs the ability to develop a comprehensive inventory of cloud computing service contracts to effectively gather, maintain, and report on cloud computing services acquired across DoD. After the DoD CIO establishes a standard, Department-wide definition for cloud computing or clarifies the NIST definition, including the five characteristics, as discussed in this report, the DoD CIO should establish an integrated repository to provide detailed information on DoD use of cloud computing services that would allow the DoD CIO to obtain information on DoD cloud computing service contracts that meet the standard definition.

DoD Could Not Measure the Effectiveness of the DoD Cloud Computing Initiative

DoD's ability to track cloud computing cost savings, and benefits is greatly limited if DoD is not aware what cloud computing service contracts exist within DoD. For example, according to the DoD CIO representatives, DoD CIO reports agency cloud spending summaries to the Office of Management and Budget (OMB). When we requested a copy of the cloud data DoD CIO reported to OMB from FY 2011 through FY 2014, DoD CIO representatives stated they feed the data directly from DoD's Select and Native Programming Data Input System for IT to OMB's IT Dash Board. DoD CIO representatives explained that DoD Components self-report the information contained in the cloud spending summaries reported to OMB. However, as discussed in this report, without a standard, Department-wide definition for cloud computing, DoD Components do not consistently identify their use of cloud computing services which affects what they self-report to the DoD CIO. In September 2014, the Council of the Inspectors General on Integrity and Efficiency (CIGIE), as part of their cloud computing initiative report,[5] concluded that all Federal agencies needed to ensure they had an accurate and complete inventory of their cloud-based systems. Establishing such an inventory would help DoD's ability to track cloud computing cost savings and benefits.

...without a standard, Department-wide definition for cloud computing, DoD Components do not consistently identify their use of cloud computing services which affects what they self-report to the DoD CIO.

[5] "The Council of the Inspectors General on Integrity and Efficiency's Cloud Computing Initiative," September 2014.

Without an accurate status of existing cloud computing service contracts, the DoD CIO cannot determine whether DoD achieves savings or gains efficiencies to measure the effectiveness of the DoD cloud computing initiative, which might impact DoD's cloud implementation efforts. In addition, without knowing what data DoD Components place on the cloud, DoD may not effectively identify and monitor cloud computing security risks. According to the CIGIE report, without accurate and complete inventories of cloud computing systems, agencies did not know the extent to which their data resided outside their information system boundaries and were, therefore, subject to the inherent risks of cloud systems. Likewise, although according to DoD CIO representatives, all DoD outsourced IT services must receive a security control review, unless DoD Components accurately classify their information systems as using cloud computing services, DoD CIO will not be aware what security risks are specific to those services.

Without an accurate status of existing cloud computing service contracts, the DoD CIO cannot determine whether DoD achieves savings or gains efficiencies...

Recommendations, Management Comments and Our Response

Recommendation 1

We recommend that the DoD Chief Information Officer:

a. **Issue guidance to either establish a standard, Department-wide cloud computing definition or clarify the National Institute of Standards and Technology definition and essential characteristics to consistently identify DoD Component cloud computing service contracts.**

DoD CIO Comments

The Principal Deputy, DoD Chief Information Officer, responding for the DoD Chief Information Officer, neither agreed nor disagreed, stating that the DoD Chief Information Officer has taken action to address the recommendation. Specifically, the Chief Information Officer published the DoD [Cloud] Computing Security Requirements Guide (CC SRG) earlier this year, which established a standard definition of cloud as well as requirements and processes for assessing cloud computing security risks. The DoD Chief Information Officer recommended closing this recommendation.

Our Response

Comments from the Principal Deputy did not address the recommendation. The CC SRG provides, among other things, guidance to DoD Mission Owners and Assessment and Authorization officials in planning and authorizing the use of a cloud service provider. The CC SRG states that it adheres to the National Institute of Standards and Technology (NIST) definition for cloud services and lists the definition, characteristics, and service models for DoD Components. However, from our review of the CC SRG, it did not establish a standard, Department-wide definition nor did it clarify to the NIST definition and characteristics of cloud computing services, which was the intent of our recommendation.

As documented in our report, the DoD CIO issued prior guidance that referred components to the NIST definition and characteristics, but each component representative interpreted the NIST definition differently including whether Information Technology services must meet all five NIST characteristics. For example, one representative specifically stated that two of the five NIST characteristics, as referenced in DoD CIO's guidance, were not clear when attempting to identify a cloud service. Therefore, the DoD Chief Information Officer should establish a standard, Department-wide definition or provide a specific interpretation of the NIST definition and characteristics that would enable DoD Components to consistently identify cloud computing contracts. We request the DoD Chief Information Officer reconsider his position on the recommendation and provide additional comments in response to the final report.

b. Establish an integrated repository that provides detailed information to identify DoD cloud computing service contracts after Recommendation 1.a of this report is completed.

DoD CIO Comments

The Principal Deputy, DoD Chief Information Officer, responding for the DoD Chief Information Officer, neither agreed nor disagreed, stating that the DoD Chief Information Officer has taken action to address the recommendation. The Principal Deputy stated that the DoD Chief Information Officer implemented enhancements to the Department's Select and Native Programming Data Input System for Information Technology (SNAP-IT) to account for the cloud budget and collect information on DoD cloud contracts. The Principal Deputy further stated that these enhancements capture additional details on DoD Cloud investments and associated cloud contracts. Lastly, the Principal Deputy indicated that the DoD Chief Information Officer issued updated budget reporting guidance to inform Components on the implementation and use of the SNAP-IT enhancements. The DoD Chief Information Officer recommended closing this recommendation.

Our Response

Comments from the Principal Deputy partially addressed the recommendation. While the Principal Deputy stated that the SNAP-IT updates would capture details on DoD Cloud investments and associated cloud contracts, the comments did not include the type of information it will collect or a description of the enhancements made to capture cloud-related investments. In addition, from our recent review of SNAP-IT, it was unclear what enhancements were made to the system. The DoD Chief Information Officer needs to establish a repository that can effectively gather, maintain, and report on cloud computing services acquired across DoD. Therefore, it is important to know the type of information SNAP-IT will collect, as well as the enhancements already added, to determine whether the actions taken meet the full intent of the recommendation. We request that the DoD Chief Information Officer provide additional comments in response to the final report.

Appendix

Scope and Methodology

We conducted this performance audit, from December 2014 through October 2015 in accordance with generally accepted government auditing standards. These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

We addressed the need for a standardized cloud computing definition and an integrated repository for cloud computing service contract information in DoD. Due to the limited number of cloud computing service contracts identified, we could not provide a sufficient answer to our announced objective.

We met with DoD CIO representatives to determine which DoD Components to select for DoD cloud computing cost-benefit analysis review. We interviewed representatives from the DoD CIO to identify DoD requirements for cost-benefit analysis. We also interviewed DISA representatives to identify DoD Components that requested cloud computing service information.

We reviewed key criteria related to IT acquisition, such as DoD Instruction 5000.02, "Operation of the Defense Acquisition System," December 8, 2008. We also reviewed cost-benefit analysis criteria, specifically, Acting DoD CIO memorandums "Use of Enterprise Information Technology Standard Business Case Analysis," October 23, 2014, and "Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services," December 15, 2014.

We requested a list from DoD CIO representatives of DoD Components that had acquired cloud computing service contracts from FY 2011 through FY 2014. We also requested information from DoD CIO and DISA representatives on the definition of cloud computing. Based on the list of DoD Components received from DoD CIO representatives, we selected the three Military Departments: Army, Navy, and Air Force as the DoD Components for our audit review.

We interviewed Army, Navy, and Air Force representatives to determine the cloud computing service contracts issued from FY 2011 through FY 2014 to obtain and review the cost-benefit analysis, if prepared. In addition, we requested information from Military Department representatives for defining cloud computing.

During interviews with Military Department representatives, the Air Force identified one operational cloud computing service contract for review. During our review, we determined a BCA was conducted for the Air Force contract in January 2015, based on the Acting DoD CIO, October 2014, BCA template guidance. Since the BCA was just recently completed, it was too early to determine whether the Air Force achieved the projected savings identified in the BCA.

Use of Computer-Processed Data

We did not use computer-processed data to perform this audit.

Prior Coverage

During the last 5 years the CIGIE and DoD Inspector General (DoD IG) issued two reports related to cloud computing. Unrestricted CIGIE reports can be accessed at https://www.ignet.gov/content/reports-publications. Unrestricted DoD IG reports can be accessed at http://www.dodig.mil/aud/reports.

CIGIE

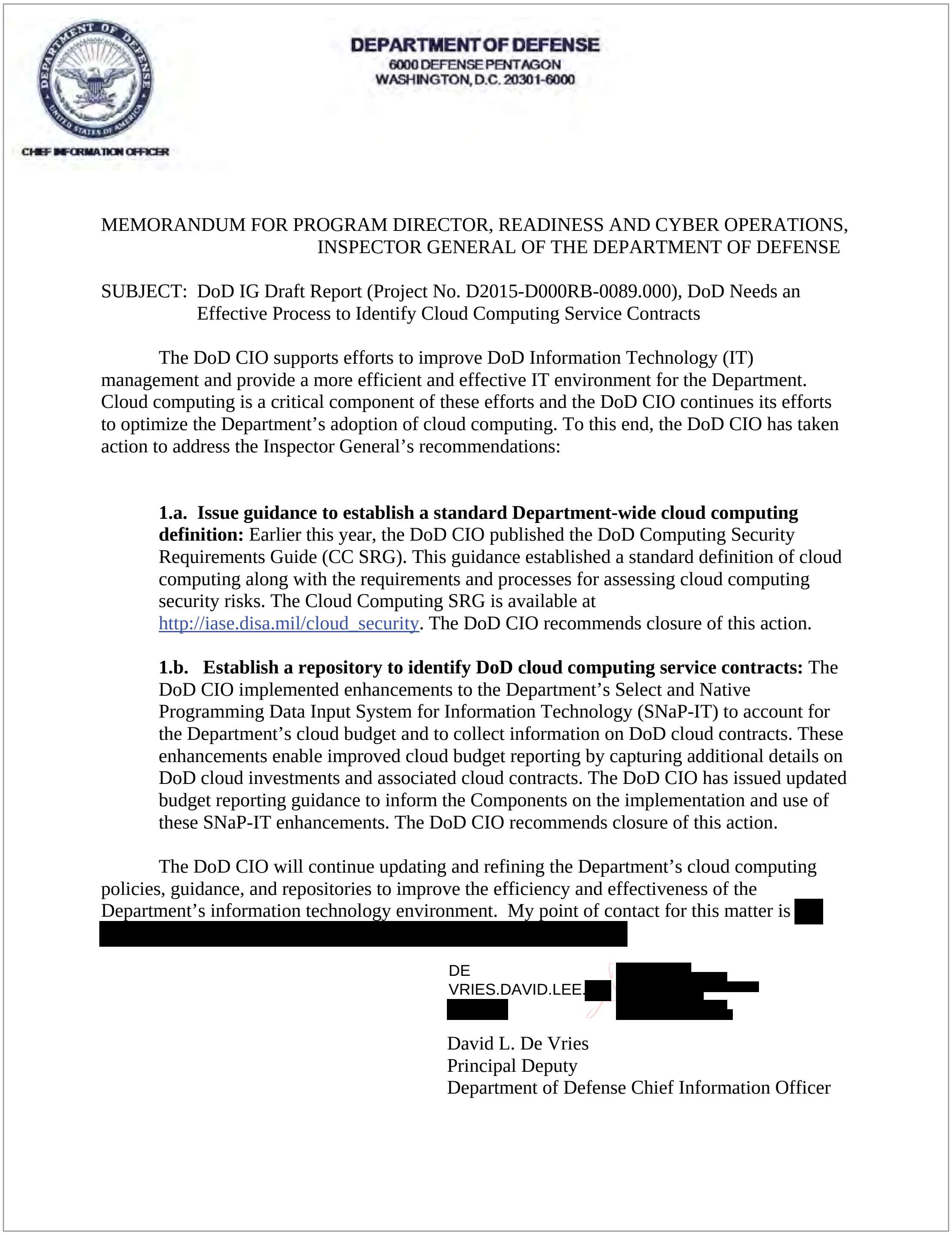
CIGIE Report, "The Council of the Inspectors General on Integrity and Efficiency's Cloud Computing Initiative," September 2014

DoD IG

DoD IG Report No. DODIG-2015-045, "DoD Cloud Computing Strategy Needs Implementation Plan and Detailed Waiver Process," December 4, 2014

Management Comments

DoD Chief Information Officer



CHIEF INFORMATION OFFICER

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

MEMORANDUM FOR PROGRAM DIRECTOR, READINESS AND CYBER OPERATIONS, INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: DoD IG Draft Report (Project No. D2015-D000RB-0089.000), DoD Needs an Effective Process to Identify Cloud Computing Service Contracts

The DoD CIO supports efforts to improve DoD Information Technology (IT) management and provide a more efficient and effective IT environment for the Department. Cloud computing is a critical component of these efforts and the DoD CIO continues its efforts to optimize the Department's adoption of cloud computing. To this end, the DoD CIO has taken action to address the Inspector General's recommendations:

1.a. Issue guidance to establish a standard Department-wide cloud computing definition: Earlier this year, the DoD CIO published the DoD Computing Security Requirements Guide (CC SRG). This guidance established a standard definition of cloud computing along with the requirements and processes for assessing cloud computing security risks. The Cloud Computing SRG is available at http://iase.disa.mil/cloud_security. The DoD CIO recommends closure of this action.

1.b. Establish a repository to identify DoD cloud computing service contracts: The DoD CIO implemented enhancements to the Department's Select and Native Programming Data Input System for Information Technology (SNaP-IT) to account for the Department's cloud budget and to collect information on DoD cloud contracts. These enhancements enable improved cloud budget reporting by capturing additional details on DoD cloud investments and associated cloud contracts. The DoD CIO has issued updated budget reporting guidance to inform the Components on the implementation and use of these SNaP-IT enhancements. The DoD CIO recommends closure of this action.

The DoD CIO will continue updating and refining the Department's cloud computing policies, guidance, and repositories to improve the efficiency and effectiveness of the Department's information technology environment. My point of contact for this matter is [redacted]

DE
VRIES.DAVID.LEE.[redacted]
[redacted]

[redacted]

David L. De Vries
Principal Deputy
Department of Defense Chief Information Officer

Acronyms and Abbreviations

BCA	Business Case Analysis
CC SRG	Computing Security Requirements Guide
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
DISA	Defense Information Systems Agency
IDIQ	Indefinite-Delivery Indefinite-Quantity
IT	Information Technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
SNAP-IT	Select and Native Programming Data Input System for Information Technology

INSPECTOR GENERAL

INTEGRITY EFFICIENCY

DEPARTMENT OF DEFENSE

Whistleblower Protection
U.S. Department of Defense

The Whistleblower Protection Enhancement Act of 2012 requires the Inspector General to designate a Whistleblower Protection Ombudsman to educate agency employees about prohibitions on retaliation, and rights and remedies against retaliation for protected disclosures. The designated ombudsman is the DoD Hotline Director. For more information on your rights and remedies against retaliation, visit www.dodig.mil/programs/whistleblower.

For more information about DoD IG reports or activities, please contact us:

Congressional Liaison
congressional@dodig.mil; 703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

For Report Notifications
http://www.dodig.mil/pubs/email_update.cfm

Twitter
twitter.com/DoD_IG

DoD Hotline
dodig.mil/hotline

DEPARTMENT OF DEFENSE | INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, VA 22350-1500
www.dodig.mil
Defense Hotline 1.800.424.9098