
Office of Inspector General

Audit Report

DOT LACKS AN EFFECTIVE PROCESS FOR ITS TRANSITION TO CLOUD COMPUTING

Department of Transportation

Report Number: FI-2015-047

Date Issued: June 16, 2015






Memorandum

U.S. Department of
Transportation

Office of the Secretary
of Transportation
Office of Inspector General

Subject: **ACTION:** DOT Lacks an Effective Process for
Its Transition to Cloud Computing
Department of Transportation
Report No. FI-2015-047

Date: June 16, 2015

From: Louis C. King 
Assistant Inspector General for Financial
and Information Technology Audits

Reply to
Attn. of: JA-20

To: DOT Chief Information Officer

The Federal Government spends about \$80 billion annually on information technology (IT). A significant portion of these funds is used to maintain aging and duplicative computer infrastructure. Cloud computing is an emerging technology that can replace aging infrastructure and help the Government improve operational efficiencies and resource use. Cloud service providers (CSP) develop infrastructures, platforms, and software application services that can be shared by multiple customers. Each customer buys the amount of service needed and can adjust the amount of service as those needs change. Government agencies enter into contractual agreements with CSPs to establish services. The Department of Transportation's (DOT) current use of cloud services includes employees' retirement and benefits self-service, contract estimating and solicitation awards, and email. When executed properly, cloud computing can provide IT services quickly and at lower costs than conventional computing but also introduces new security risks.¹

DOT's Office of Inspector General (OIG) joined the Council of Inspectors General on Integrity and Efficiency's project to determine the status of Federal agencies' cloud computing environments. Consistent with the CIGIE project, our audit objectives were to determine whether DOT (1) has an effective process to transition IT services to cloud

¹ GAO, *Additional Guidance Needed to Address Cloud Computing Concerns*, GAO-12-130T.

computing, and (2) has identified and mitigated security risks associated with the transition. We conducted our work in accordance with generally accepted Government auditing standards. This report presents our review of 6 DOT cloud systems. See exhibit A for details on our scope and methodology.

RESULTS IN BRIEF

DOT has taken steps to transition to cloud computing, such as establishing a multi-modal Cloud Working Group. Still, the transition has not been effective because the Department has not established guidance on contracting for cloud systems or for cost and benefit assessments of the systems. In addition, the Department has not updated its guidance on contracting for IT services to include cloud systems. Consequently, the guidance does not include requirements for specific contract clauses needed for cloud services, such as provisions that cover maintenance of data integrity, availability, and confidentiality. Some of these provisions—needed to ensure that CSPs keep agencies' data secure and available when needed—are lacking in each of the Department's cloud contracts. For example, three of the six contracts we reviewed did not include provisions establishing non-disclosure agreements required to protect agency information from inappropriate release. Additionally, the Department has not established standards for assessing the costs and benefits of cloud systems. Consequently, the Operating Administrations cannot determine whether moving to the cloud is cost effective and could achieve the expected benefits.

DOT's risk management and oversight of its cloud systems are also ineffective. The Department has not established an accurate inventory of cloud systems—a requirement for effective information system risk management. Although the Department reported 14 cloud systems to us, we determined that only 11 were actually cloud systems. Furthermore, of these 11 systems, only 5 were correctly identified in the Department's inventory. Four were identified as non-cloud systems, and 2 were not in the inventory at all. As a result of the inaccurate inventory, officials that authorize the use of cloud systems lack information needed to make informed decisions. Furthermore, the Department's cloud systems did not meet the requirements of the Federal Risk Authorization and Management Program (FedRAMP). FedRAMP provides a standardized approach for each Operating Administration security assessment of cloud systems and authorization of their use. The Program required security at all Federal cloud systems to be compliant with its guidelines by June 2014.

We are making recommendations to the Department to help improve contracts covering cloud computing and the Department's oversight of the transition.

BACKGROUND

In December 2010, the Administration established a cloud first policy in the *25 Point Implementation Plan to Reform Federal Information Technology Management*.² Under this policy, Federal agencies are required to procure cloud-based solutions whenever secure, reliable, cost-effective cloud options exist.

OMB established FedRAMP in 2011³ to provide a standardized approach to each Operating Administration's security assessments and authorizations of cloud systems. Authorization is the process by which a senior management official reviews a system's security related information and determines if the risk of operating the system is acceptable. If so, the senior official grants an authority to operate the system. FedRAMP's process and requirements include:

- A Joint Authorization Board that defines and updates FedRAMP security authorization requirements, approves criteria for Federal agencies' assessments of CSPs, and reviews CSPs' requests for authorization to provide services to Federal agencies.
- A Program Management Office that maintains a process for agencies to adhere to the Board's security authorization requirements.
- A requirement that departments use FedRAMP when conducting risk assessments, security authorizations and granting authority to operate to all cloud services.

Under FedRAMP's guidelines, all cloud systems procured after April 2012 must be FedRAMP compliant. Systems that were in operation prior to April 2012 were grandfathered in until June 2014.

In a December 2011 memorandum, the Federal Chief Information Officer required that Executive Departments establish processes to support privacy and security for cloud systems. The Federal Chief Information Officers Council and Chief Acquisition Officers Council have also established requirements⁴ for cloud computing contracts that call for the Federal agency and CSP to agree in the contract on:

- The services the agency needs;
- The cost of each service;
- A method for measuring the amount of service used and the associated costs;
- The level of protection for the agency's information; and
- The agency's and the CSP's roles and responsibilities.

² www.cio.gov.

³ OMB Policy Memo, Security Authorization of Information Systems in Cloud Computing Environments, December 8, 2011.

⁴ Federal CIO Council and Chief Acquisition Officers Council, *Creating Effective Cloud Computing Contracts for the Federal Government: Best Practices for Acquiring IT as a Service*, February 2012.

The Councils' requirements also state that the contracts should include language that covers:

- Non-disclosure agreements, which Federal agencies require to protect sensitive information from public disclosure by CSPs;
- Acceptable service levels and performance standards, which detail the uptime of services to customers, the process and definition of calculating and measuring uptime, and the way in which the agency will receive credits in the event that the CSP fails to meet its contractual uptime requirements; uptime is the amount of time that cloud systems and services are accessible by customers;
- Electronic discovery—or e-discovery—requests from opposing parties involved with Federal agencies in litigation. Agencies require that information relevant to law suits be stored separately from non-relevant information in order to maintain chains of custody. Contracts for cloud computing services should define how CSPs will address these requirements should they arise;
- Data management and handling requirements, including data preservation and privacy maintenance;
- Identification of responsibilities in the event of data loss or information breach;
- Specific language required under the Federal Acquisition Regulation (FAR) for Federal contracts for procurement of goods and services.

DOT's policy,⁵ based on the National Institute of Standards and Technology's (NIST) guidelines, also calls for maintaining an accurate inventory of the Department's information systems, including cloud systems. The Department's inventory is located in the Cyber Security Assessment and Management (CSAM) database.

DOT IS NOT EFFECTIVELY TRANSITIONING TO CLOUD SYSTEMS

The Department recognizes its need to improve its transition to cloud systems. To address this, the Department has, among other things, established a Cloud Working Group comprised of key procurement and information technology representatives from across the Department. Still, DOT's transition to cloud computing has not been effective because the Department has not updated its guidance on contracting for IT services with requirements for cloud services contracts, or established procedures for costs and benefits assessments of cloud systems. The Operating Administration contracts for cloud services lack provisions on several requirements for cloud services and system security, and the Department has not conducted cost benefit analyses of the systems that are in place.

⁵ DOT FISMA Inventory Guide, 2012.

DOT's Contracts for Cloud Services Lack Provisions on Services and Security

All of the Department's cloud services contracts lack provisions on information integrity, availability, and confidentiality that the Federal Information Officers' and Acquisition Officers' Councils state they should include. For example, only FHWA's contract specifies data uptime requirements. This same contract, however, lacks a provision that defines a methodology for uptime calculations. Furthermore, none of the contracts includes requirements regarding e-discovery requests. Three contracts lacked clauses that the Federal Acquisition Regulation (FAR) requires covering contractors' disclosure of information to law enforcement, and only two specifically granted inspectors general access to examine records. See table 1 for a summary of contract provisions. For example, the table indicates that three of the six contracts we reviewed did not include provisions establishing non-disclosure agreements required to protect agency information from inappropriate release in the "Confidentiality" section.

Table 1. Provisions on Confidentiality, Data Integrity, Availability, and Other Clauses in Six Cloud Services Contracts

Contract provision: Contract number		NHTSA (1)	FHWA (2)	FHWA (3)	FRA (4)	FRA (5)	OST (6)
Confidentiality	Includes CSP's signed non-disclosure agreement to protect non-public information.	✓	✓	✓	○	○	○
	Establishes rules of behavior regarding non-disclosure and a method for monitoring behavior.	○	○	✓	○	○	○
Integrity	Is FedRAMP compliant?	○	○	○	○	○	○
	Includes specific, detailed responsibilities in a system security plan.	○	○	○	-	○	✓
Availability	Specifies uptime requirements.	○	○	✓	○	○	○
	Defines methodology for uptime calculations	○	○	○	○	○	○
	Specifies Operating Administration's monitoring of uptime to ensure compliance and/or pursue credits if uptime targets missed.	○	○	○	○	○	○
Other	Address procedures for e-Discovery requests	○	○	○	○	○	○
	Contractors disclosure to law enforcement	✓	○	○	○	✓	✓
	Inspectors General access to examine records	✓	✓	○	○	○	○

✓ = included in provision
Source: OIG analysis

○ = missing from provision

- = not applicable

The lack of departmentwide procedures for procuring cloud services results in contracts for cloud services that do not guarantee the protection and integrity of DOT's information.

DOT Has Not Established Procedures for Costs and Benefit Assessments of Cloud Systems

DOT does not have procedures for assessing cloud systems' costs and benefits. To comply with the Administration's cloud first policy, departments must determine the cost effectiveness of cloud systems prior to establishing them. OMB's Circular A-11 establishes a process for analyzing costs and benefits of cloud systems. However, DOT

has not established procedures for implementing OMB's process, and we found no evidence that the Operating Administration using cloud systems had done this analysis. This lack of cost benefit analyses of cloud computing makes it difficult for the Operating Administrations and the Department to determine whether cloud computing helps the Department save Federal dollars or improve services.

DOT's RISK MANAGEMENT AND SECURITY OVERSIGHT OF ITS CLOUD SYSTEMS ARE INEFFECTIVE

DOT's risk management and oversight of its cloud systems are also ineffective. The Department has not established an accurate inventory of cloud systems—a requirement for effective information system risk management—and officials that authorize cloud system use lack information to make informed decisions. Furthermore, the Department's cloud systems were not FedRAMP compliant.

DOT's Risk Management of its Cloud Systems Is Ineffective because its System Inventory Is Inaccurate

NIST's guidance states that effective risk management requires complete inventories and categorizations of information systems. DOT has guidance⁶ on inventory documentation for cloud systems and authorization of their use that requires Operating Administrations to accurately categorize cloud systems and indicate whether a cloud resource is FedRAMP compliant. The Operating Administrations reported having 9 cloud computing systems, but we found that only 6 of these 9 were actually cloud systems. The Department later reported an additional 5 cloud systems. However, only 11 of the 14 cloud systems that Department and the Operating Administrations reported to us were actually cloud systems. Furthermore, of these 11 systems, we found that only 5 were correctly identified in CSAM. Four were identified as non-cloud systems, and 2 were not in CSAM at all.

An inaccurate inventory makes it difficult for the Department to provide direction to Operating Administrations and contractors on information security, to enforce compliance with information security requirements, and to ensure security risks are reduced in cost effective ways.

Authorizing Officials Do Not Have Complete Information about Cloud Systems

Authorizing officials are senior officials at each Operating Administration that accept the risks associated with information systems, and authorize their use. Because DOT has not provided guidance on how to make cloud systems FedRAMP compliant, authorizing

⁶ DOT FISMA Inventory Guide, June 2012.

officials may not have enough information regarding a system's risks and needed security controls. For example, authorizing officials authorized four systems for use without documentation that they were cloud systems because the Operating Administration had provided them incomplete information on the systems. Furthermore, two systems were part of group authorizations that included non-cloud systems, but there was no indication for the authorizing official that the group contained cloud services. One authorized system was part of DOT's common operating environment (COE). According to the Department, the cloud system in the COE has not had a complete security assessment and authorization. OST self-assessed the cloud service and found that 57 percent of the contract provisions evaluated was not included in the system's contract.

DOT's Cloud Systems Were Not FedRAMP Compliant as of June 2014

None of the Operating Administrations cloud systems were compliant with FedRAMP's requirements. FedRAMP's guidance requires that a specific set of security controls be implemented and that the responsibility for each—agency personnel or CSP—be specified. Federal Highway Safety Administration implemented the required security controls but has not specified which party is responsible for each control's actions. In addition, four CSP's security controls did not undergo independent assessments at DOT by a FedRAMP approved third party. Consequently, FedRAMP's Joint Authorization Board has not authorized use of these cloud systems.

Because DOT's cloud systems do not meet FedRAMP's security controls, Federal data are at risk for compromise, corruption, or loss. Furthermore, the Department may be operating cloud systems without adequate understanding of the risks.

According to officials in the Office of the Chief Information Officer (OCIO) as part of its response to a recommendation on cloud computing in OIG's 2013 Federal Information Security Management Act (FISMA) report, the Department is developing requirements and guidance for transitioning to cloud services as part of a collaborative transition project. OCIO's and the Operating Administration acquisition officials are participating in the project under FAA's leadership.

CONCLUSION

The Federal Government is moving to cloud computing to increase efficiency and to save taxpayer funds. DOT has begun moving in this direction. However, the cloud computing environment can expose sensitive Government information to the risk of compromise unless effective security and management controls are implemented. Additionally, DOT cannot have assurance that implementing cloud systems is cost-beneficial.

RECOMMENDATIONS

To help improve the Department's transition to cloud based computing, we recommend that OCIO:

1. Develop guidance for acquisition of cloud services, cost and savings analysis, and operational support for use of those services.
2. Develop a process to verify that non-disclosure agreements and language regarding discovery and investigatory access requirements are included in future cloud contracts.
3. Establish procedures to verify cloud systems are accurately inventoried in CSAM.
4. Establish FedRAMP compliance guidelines and oversight for the Department, and ensure that each Operating Administration put plans in place to meet FedRAMP requirements.

AGENCY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

We provided OCIO with our draft report on April 23, 2015, and received its response on May 28, 2015, which is included as an appendix to this report. The Department concurred with our four recommendations and provided appropriate actions and completion dates. Accordingly, we consider all recommendations resolved but open pending completion of the planned actions.

ACTIONS REQUIRED

We consider all four recommendations resolved but open pending completion of planned actions.

We appreciate the courtesies and cooperation of OST representatives during this audit. If you have any questions concerning this report, please call me at (202) 366-4350, or Nathan Custer, Program Director, at (202) 366-5540.

#

cc: DOT Audit Liaison, M-1

EXHIBIT A. SCOPE AND METHODOLOGY

We conducted this audit from January 2014 through April 2015 in accordance with generally accepted Government auditing standards. Those 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

OIG joined with 18 other Inspectors General to support CIGIE's IT Committee's governmentwide initiative to evaluate participating agencies' efforts associated with adopting cloud computing technologies.

Our review of the security and controls over DOT cloud services focused on whether DOT (1) has an effective process to transition IT services to cloud computing, and (2) has identified and mitigated security risks associated with the transition.

To conduct our work, we surveyed DOT and its Operating Administrations for public cloud services that were in production during and after December 2013. For those cloud systems identified, we followed up and requested the associated contract documents for the systems. DOT reported 9 cloud systems in production in the following Operating Administrations: Federal Highway Administration, National Highway Traffic Safety Administration, Federal Railroad Administration, Pipelines and Hazardous Materials Safety Administration, and the Office of the Secretary of Transportation, Office of Research and Technology.

We used CIGIE's evaluation criteria to analyze the nine cloud services. In these analyses, we reviewed administrative details and 7 performance areas, including: (1) Roles and Responsibilities; (2) Service Level Agreements; (3) Access; (4) Monitoring; (5) Enterprise Management; (6) FedRAMP Compliance; and (7) FedRAMP Follow-up. To validate DOT's process to transition to cloud systems, we evaluated the effectiveness of Roles and Responsibilities, adequacy of Service Level Agreements, Access, Monitoring and Enterprise Management. To determine whether the Department was identifying and mitigating security risks, we evaluated the Operating Administrations' compliance with FedRAMP's process.

We interviewed individuals from the Operating Administrations and OCIO, and the Contract Officers that were associated with the systems and procurements. We analyzed information for each of the 9 systems. We shared our analyses with the Operating Administrations for concurrence and to ensure accuracy.

Since we had determined that the Department did not maintain an accurate inventory of cloud computing investments,⁷ we reviewed the Department's May 2014 submission to OMB of its Quarterly E-Government Integrated Data Collection, known as the Portfolio Stat. This Portfolio Stat contained information on the Department's use of cloud systems. We found discrepancies between what the Department reported to OMB and the cloud systems that the Department reported in our survey for this audit. We requested clarification from the Department's interim Chief Information Security Officer. As a result of our request, the Department changed the list of systems that it classified as cloud systems.

Of the original 9 systems identified in the audit survey, we found that only 6 were actually cloud systems. This report presents our review of these 6 systems. The Department later reported an additional 5 cloud systems for a total of 11, but we considered review of 6 systems to be sufficient, and therefore, did not review the other 5.⁸

We forwarded to CIGIE for use in its report the list of cloud services identified, certain budget and administrative information, and the technical analysis of those systems.⁹ Our findings were consistent with those that CIGIE presented in its report.

⁷ *DOT Has Made Progress but Significant Weaknesses in Its Information Security Remain*, OIG Report Number FI-2015-009. OIG's reports are available at www.oig.dot.gov.

⁸ PHMSA's two systems and FRA's one system were removed from our analysis. FAA had three systems added, and OST and FMCSA each had one system added.

⁹ *The Council of the Inspectors General on Integrity and Efficiency's Cloud Computing Initiative*, September 2014.

EXHIBIT B. MAJOR CONTRIBUTORS TO THIS REPORT

Name	Title
Nathan Custer	Program Director
James Mullen	Information Technology Specialist
Shavon Moore	Information Technology Specialist
Fritz Swartzbaugh	Associate Counsel
Petra Swartzlander	Senior Statistician
Susan Neill	Writer / Editor
Tom Denomme	Project Consultant

APPENDIX. AGENCY COMMENTS

U.S. Department of
Transportation

Office of the Secretary
of Transportation

Memorandum

Subject: **INFORMATION**: Management Comments – Office of Inspector General Date: **MAY 28 2015**
(OIG) Draft Report on DOT Cloud Computing

From: Richard McKinney
Chief Information Officer (CIO)

A handwritten signature in blue ink, appearing to read "Richard McKinney", with a long horizontal line extending to the right.

To: Louis King
Assistant Inspector General for Financial
and Information Technology Audits

The Department of Transportation's (DOT) successful implementation of cloud services was made possible by leveraging savings from the ongoing maintenance of outdated systems to the retirement of those systems. The use of cloud services improves mission and business effectiveness and increases operational information technology (IT) efficiencies. To further increase savings, DOT established a cloud working group that strategically focuses on four principal areas:

1. Adopt Cloud Governance and Management Practices
2. Implement Cloud Computing Capabilities
3. Manage the Modernization and Migration of Applications, Systems and Data
4. Secure and Manage Cloud Operations

The Office of the Chief Information Officer (OCIO) reviewed the draft report and offers the following comments in response to OIG's findings and recommendations:

- OCIO will continue to leverage the Cloud Working Group and drive changes identified in the report with the support of representatives from the Operating Administrations, key procurement offices, and IT offices.
- Utilizing the knowledge identified by the Cloud Working Group, the OCIO will update its processes, guidance, and oversight plans and to ensure Federal compliance. Current OCIO policy, based on the National Institute of Standards and Technology (NIST), outlines the maintenance and accurate inventory of DOT's information systems, including cloud systems.

Based upon our review of the draft report, we concur with OIG recommendations 1 – 4, as written. We plan to implement recommendation 2 by October 30, 2015 and recommendation 3 by December 31, 2015. Recommendations 1 and 4 will be completed by May 15, 2016.

Appendix. Agency Comments

We appreciate the opportunity to review and respond to the report. If you have any questions concerning the response, please contact Jason Gray, Associate Chief Information Officer for IT Policy and Oversight, at (202) 366-2498.