National Science Foundation • Office of Inspector General
4201 Wilson Boulevard, Suite I-1135, Arlington, Virginia 22230

MEMORANDUM

DATE: December 3, 2015

TO: Amy Northcutt
Chief Information Officer

FROM: Dr. Brett M. Baker
Assistant Inspector General for Audit

SUBJECT: *Cloud Computing Inspection,* Report No. 16-3-003

Attached please find the final report of our inspection of NSF's implementation of cloud computing technologies. The report contains three findings to: 1) maintain an accurate cloud system inventory; 2) include more detailed specifications in contracts for cloud services; and 3) meet FedRAMP requirements. We have included NSF's response as an appendix to the final report.

In accordance with OMB Circular A-50, Audit Follow-up, please provide our office with a written corrective action plan to address the report's recommendations. In addressing the report's recommendations, this corrective action plan should detail specific actions and associated milestone dates. Please provide the action plan within 60 calendar days of the date of this report.

We appreciate the courtesies and assistance provided by NSF staff during the inspection. If you have any questions, please contact Thomas Moschetto, Director, Financial and IT Audits, at (703) 292-7398.

Attachment

cc:
Richard Buckius
Dorothy Aronson
Gregory Steigerwald
Nick Ipiotis
Daniel Hofherr
Mary Lou Tillotson
Rafael Cotto
Fae Korsmo
Christina Sarris
Michael Van Woert
Ruth David, NSB
Allison Lerner
Louise Nelson
Thomas Moschetto
Emily Franko
Brian Gallagher

Cloud Computing Inspection

National Science Foundation
Office of Inspector General

December 3, 2015

OIG 16-3-003

Introduction

The National Science Foundation (NSF) is an independent federal agency created by the National Science Foundation Act of 1950 (P.L. 81-507). Its mission is “to promote the progress of science; to advance the national health, prosperity, and welfare; and to secure the national defense.”

Federal agencies were mandated in 2011 by the U.S. Chief Information Officer’s ‘cloud first policy’[1] to evaluate safe and secure cloud computing options when making new IT investments, which resulted in an increased investment in cloud technologies by NSF.

Cloud Computing Technology

Cloud computing refers to information technology systems, software, and infrastructure that a service provider packages and sells to consumers. The National Institute of Standards and Technology (NIST) 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. Cloud computing is composed of five essential characteristics:[2]

- 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 substantial 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, build, and maintain hardware or data centers necessary for maintaining in-house information systems.

However, utilization of cloud systems presents additional risks unique to such a set-up, such as loss of control over the data, security, and access issues that need to be properly managed by federal agency consumers. These risks can be mitigated by taking precautionary and proactive steps, such as negotiating contractual provisions, to protect the data, interests, and resources of the Federal Government.

NSF must therefore balance the cost savings benefit of cloud technology with the risks involved in ceding control over agency data and systems to a commercial entity in a cloud environment.

[1] Kundra, V., *Federal Cloud Computing Strategy*, February 8, 2011.
[2] NIST Special Publication (SP) 800-145, *The NIST Definition of Cloud Computing*, September 2011.

Objectives

The objectives of this review were to evaluate NSF's efforts to adopt cloud-computing technologies and to review executed contracts between the agency and cloud service providers for compliance with applicable standards.

The Division of Acquisition and Cooperative Support (DACS) within NSF's Office of Budget, Finance & Award Management is responsible for managing the business and non-technical aspects of contract acquisition for the agency, including contracts for cloud computing services. The Division of Information Systems (DIS) within NSF's Office of Information & Resource Management is responsible for providing the agency full life-cycle information technology support and assuring the availability, accessibility, security, and integrity of NSF information and services.

NSF reported that it had four cloud service contracts, ranging from three to five years in length, valued at approximately $27.8 million[3] as of February 25, 2015. We selected the following three for review:

- External SharePoint hosted by Amazon Web Services via DLT (Reseller of licenses) for $468,510
- Office 365 E-mail provided by Microsoft Corporation via GovConnection (Reseller of licenses) for $2.42 million
- iTRAK Financial Management System provided by Accenture Federal Services for $24.48 million

A diagram illustrating the relationships among the main parties involved for each of the three contracts reviewed is provided in Appendix C.

This review began as part of a Council of Inspectors General on Integrity and Efficiency (CIGIE) government-wide initiative to look at cloud-computing environments within the Federal Government. Due to resource constraints, the inspection was put on hold, and completed after CIGIE issued its consolidated cloud computing initiative report.[4] The NSF Office of Inspector General (OIG) review team followed the CIGIE Cloud Computing Collaboration Matrix steps to complete this inspection. However, the applicability of each question in the standardized matrix of questions varied by contract.

[3] Excluded from this figure are the three cloud service contracts NSF omitted, totaling $694,465, as discussed in the first finding.

[4] *CIGIE Cloud Computing Initiative Report*, September 2014.

Results

As a federal agency consumer that is increasing its reliance on cloud computing technologies, NSF has developed some effective oversight procedures consistent with cloud best practices, such as assigning an agency official to monitor the Cloud Service Provider's (CSP's) compliance with contractual terms, obligations, and performance metrics; realizing cost savings from the competitive bidding process; and incorporating certain language and FAR clauses into the cloud contracts and related agreements that protect the agency's interests. Also, NSF is using Federal Risk and Authorization Management Program (FedRAMP) approved CSPs for two of the three contracts reviewed, and is actively working with the other CSP to pursue FedRAMP approval.

Despite the development of these oversight procedures, we found that NSF has not consistently implemented these procedures across all of its cloud contracts. Although each of the three contracts tested contained some of the cloud best practice elements, no one contract included all of the best practices.

NSF should strengthen its governance of cloud computing services, and better address business and security risks by improving its inventory management of cloud services, including more detailed specifications in its cloud contracts, and requiring compliance with FedRAMP requirements for all of its cloud services.

Finding 1 - NSF Should Maintain an Accurate Cloud System Inventory

During the course of performing this inspection, we determined that NSF's Division of Information Systems (DIS) did not have an accurate and complete inventory of NSF's cloud services and providers. We found that DIS does not know all the cloud services acquired and operating at NSF because the agency did not have a process in place to centrally capture, manage, and report on this information. Without an accurate and complete inventory, the agency does not know the extent to which its data resides outside its own information system boundary, which subjects this data to risks inherent with cloud systems. These risks, which include interception of data in transit, unsecure storage, and ineffective deletion of data, could expose the agency's data to unauthorized parties and potentially compromise the objectives of NSF's programs. Further, according to ISACA,[5] having an enterprise-wide inventory of cloud-computing services and providers is a best practice that helps organizations ensure they do not use unapproved or unsecured services.

As part of our inspection, we asked DIS for an NSF-wide inventory of deployed cloud services and associated service providers. We found that DIS did not report at least three of seven NSF cloud service contracts, with contract values totaling $694,465, which should have been included in its February 2015 cloud services inventory submission to OIG. In July 2015, OIG inquired about two cloud services known

[5] Previously known as the Information Systems Audit and Control Association, ISACA now goes by its acronym only to reflect the broad range of IT governance professionals it serves. ISACA is a global organization engaged in the development and adoption of widely accepted, industry-leading practices for information systems.

to exist at NSF prior to February 2015, but which had not been included in the February 2015 submission. DIS subsequently reported eight total cloud service contracts, or four additional cloud service contracts than previously reported to us in February 2015. Three of these four new cloud service contracts were effective in 2014, and therefore should have been included as part of the February 2015 cloud services inventory submission.

The Office of Management and Budget (OMB) requires federal agencies to follow NIST guidance.[6] According to NIST,[7] 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.

Recommendation: We recommend that NSF implement a process to consistently, accurately, and completely report on and manage its cloud services to maintain a current inventory.

Finding 2 – NSF Should Include More Detailed Specifications in Its Cloud Contracts

We found that all three cloud contracts in our sample did not contain detailed specifications for the agency and the CSP to adhere to, including adequately defined Service Level Agreements (SLAs), Non-disclosure Agreements (NDAs), data preservation responsibilities, federal regulation requirements, and audit and investigative access in all cloud contracts and services acquired. Although each of the contracts tested did contain some of the best practice elements, no one contract included all of the elements. This occurred because NSF lacks a standardized strategy and approach to acquiring cloud services, that would include a standard set of requirements that CSPs must adhere to when providing cloud services to NSF. When utilizing a cloud system, the customer cedes control to the CSP on a number of issues that may affect the system's security. Consequently, without detailed contract specifications addressing these consumer needs and effective risk management processes, NSF's data stored within the cloud environment is at risk.

For two of the three NSF contracts we reviewed (Office 365 and Amazon Web Services), NSF purchased (standardized) commercially available off-the-shelf[8] product licenses off of a government-wide master contract via resellers.[9] NSF accepted the cloud providers' standard service contract for these two cloud

[6] OMB M-14-04, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, November 18, 2013.
[7] NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013.
[8] Commercially available off-the-shelf, or Commercial off-the-shelf, items are defined as any item of supply that is (i) a commercial item; (ii) sold in substantial quantities in the commercial marketplace; and (iii) offered to the Government, under a contract or subcontract at any tier, without modification, in the same form in which it is sold in the commercial marketplace.
[9] While we recognize that there are various methods to acquire cloud services, and related implications to consider when evaluating cloud computing technologies, the purpose of this inspection was to evaluate contracts between

services. For contracts involving the purchase of licenses for commercial off-the-shelf products, NSF officials stated they have little bargaining power to negotiate the manufacturer's commercial marketplace terms of service.

Regarding consumer needs, the Chief Information Officers (CIO) Council and the Chief Acquisition Officers (CAO) Council issued a cloud computing best practices paper[10] (cloud best practices) that provides specific guidance on how federal agencies should effectively procure cloud services within existing laws and regulations. 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 agreements address time requirements that a CSP must follow to comply with federal agency rules and regulations. This includes complying with statutory requirements and associated deadlines such as those found under FISMA and FOIA, and applicable regulatory structures, such as those governing Inspector General (IG) investigations and audits. 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 metrics. Further, per NIST SP 800-144,[11] 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.

Specific details by CSP/Contract are included in the following table:

agencies and cloud service providers to determine whether applicable standards, such as cloud best practices, had been appropriately implemented.

[10] 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.

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

Table: Review of NSF Contracts with Cloud Service Providers (CSPs)

	Cloud Contracts		
Contract Has (Had) Provisions Addressing	**AWS/DLT External SharePoint (Commercial Off-the-Shelf Licenses)**	**Microsoft/ GovConnection Office 365 Email (Commercial Off-the-Shelf Licenses)**	**Accenture Federal Services iTRAK Financial Management System**
Roles and Responsibilities Defined in Contracts			
Defined roles and responsibilities of all parties (agency, CSP, and end users)	Yes	Yes	No – Note (1)
Timeframes that the CSP will need to follow in order to comply with federal agency rules and regulations[12]	No	No	No
Non-disclosure agreements (NDAs) signed by CSP and/or CSP non-disclosure language in contract documentation protecting agency data	No – Note (2)	Yes	Yes
Monitoring of CSP and/or end user compliance with NDA (or Non-disclosure terms)	N/A	No	No
Service Level Agreements (SLAs) in Contracts			
Stated minimum system availability level requirements (uptime)	Yes	Yes	Yes
Reporting of service level metrics (to NSF)	Yes	Yes	Yes
Compensation (service credits) available to agency for CSP not meeting service levels	No	Yes	No
Access to CSP for Audit and Investigative Purposes			
Language allowing OIGs full and unrestricted access to the contractors' (and subcontractors') facilities, installations, operations, documentation, databases, and personnel used in performance of the contract in order to conduct audits, inspections, investigations, or other reviews	No	No	Yes

[12] Per cloud best practices, contract provisions regarding law, jurisdiction, and indemnification arising out of a federal agency's use of a CSP environment must align with federal statutes, policies, and regulations; and compliance should be defined before a contract is awarded.

e-Discovery procedures addressed	No	No	No
Agency Process for Monitoring its Cloud Computing Provider			
Department/Agency Official *Assigned* to Monitor Compliance with Contract/Terms of Service (TOS)/Service Level Agreement (SLA)	Yes	Yes – Note (3)	Yes
Department/Agency Official Actually Monitoring Contract/TOS/SLA	Yes	No – Note (4)	Yes
Method to monitor end-user activities in the cloud environment	No	No	No
Data Management			
Data preservation responsibilities, and data retention and destruction (deletion) addressed	Yes	Yes	No – Note (5)
Data preservation[13] clauses adequately protect the agency's interests and data in the event the contract is terminated *for cause*	No	Yes	No
Notes (1) The contract documentation, including the Terms of Service (TOS), does not detail how the end users may use the services. Roles and responsibilities of the agency and CSP are defined. (2) NSF officials stated that NSF is responsible for access control and encryption for this cloud service, and the CSP can't access the cloud environment, or the data within it. Therefore, NDAs signed by the CSP and non-disclosure terms in the contract were not needed. (3) No NSF official is assigned to monitor end users' compliance with TOS. An agency official has been assigned to monitor agency and CSP compliance with the TOS, SLA and other contract terms. (4) NSF officials told us they rely on end-users to report connectivity, outage, and other issues as they arise. (5) Per NSF, this will be negotiated as part of Transition Services at (near) contract expiration or termination.			

The nature of cloud computing requires customers to relinquish varying levels of control of their data and information to CSPs. By not negotiating with the cloud providers on service level and terms of service agreements; not requiring the cloud providers to sign NDAs; and not monitoring end users' and cloud providers' activity in the cloud environment, the confidentiality, integrity, and availability of NSF's data could be compromised. Additionally, when the agency relies on end users to report outages and inappropriate disclosure of sensitive information, and does not monitor the CSP's performance and ability

[13] NIST SP 800-146 discusses 'data preservation' responsibilities in the context of how long the CSP must maintain the agency's data in the event the contract is terminated '*for cause*'.

to meet required service levels and contractual requirements, the risk that NSF's resources will be used inappropriately or ineffectively is increased.

Service Level Agreement (SLA)

SLAs define the acceptable level of service the CSP will deliver in measurable terms, the service credit (compensation) available to the consumer if the CSP fails to deliver at the specified level, and outline consumer obligations in obtaining such remedies.[14] We found that two of the three contracts reviewed did not provide service credits or other remedies to the agency for the cloud provider failing to meet agreed-upon service levels, and the NSF official assigned for the other contract was not monitoring the cloud provider to ensure its service level obligations were met. If NSF does not establish a service credit or other consequence for the CSP failing to perform at required levels, there is less of an incentive for CSPs to meet requirements, resulting in potential ineffective use of NSF's resources. Further, if NSF does not monitor and verify the uptime percentages, it cannot be assured that it will receive a service credit remedy if the CSP does not meet its 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. It asserts 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. NIST SP 800-146 also 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. Also, NIST states that an agency should understand both its responsibilities and those of the CSP before using a cloud service.

Data Preservation

We found that one of the three contracts did not address data preservation responsibilities in terms of defining how long the CSP must maintain the agency's data in the event the contract is terminated or expires. NSF stated such terms would be negotiated closer to contract expiration or transition. For another contract, NSF was not adequately protected by data preservation clauses as the contract does not specify how long the CSP would maintain NSF data, the deletion process, nor costs involved to retrieve data in the event that either party terminates the contract for cause.

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.[15] By not clearly and adequately specifying data preservation responsibilities, processes, and related costs to access data upfront in the initial contract, there is a risk that NSF could experience costly outages, delays in service, and limited access to data at contract expiration or termination. This could also result in NSF incurring additional fees for services at or around the time of contract termination, expiration, or transition to a subsequent contractor.

Non-Disclosure Agreement (NDA)

We found that for the two contracts in which NSF acquired licenses via resellers, the cloud computing provider did not sign a NDA to protect non-public information that is protected by privacy laws (such as

[14] NIST SP 800-146, *Cloud Computing Synopsis and Recommendations*, May 2012.

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

the Privacy Act of 1974), procurement-sensitive, affects pre-decisional policy, physical security, or other information deemed important to protect. One of these two contracts had sufficient language to protect NSF data and satisfy the intent of the best practice, but the other did not. For all three contracts reviewed, NSF did not monitor the contractor's compliance with the NDA or whether agency data had been improperly disclosed.

Because CSP personnel have access to, and control of the federal data residing in the cloud system, NDAs are a critical control to ensure cloud providers protect the information stored in the cloud. Moreover, cloud best practices state that federal agency oversight over NDAs should include examining non-disclosure agreement requirements included in the Rules of Behavior and monitoring end-users activities in the cloud environment. The Rules of Behavior (typically related to and contained in NDAs), which are required by 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.[16]

Access to CSP for Audit and Investigative Purposes

We found that two of the three contracts did not include Federal Acquisition Regulation (FAR) clause 52.239-1[17] or CIGIE-recommended language permitting the Agency and OIG full and unrestricted access to the contractors' (and subcontractors') facilities, installations, operations, documentation, databases, and personnel used in performance of the contract in order to conduct audits, inspections, investigations, or other reviews.[18] Under FAR clause 52.203-13, which was included in both of these contracts, the contractor is required to provide full cooperation for audits, investigations, and corrective actions. This gives OIGs access to documents and employees in response to OIG requests. However, it does not give OIGs the full and unrestricted access provided by FAR clause 52.239-1 and the CIGIE-recommended language (see above), which is much broader (including, e.g., access to databases and facilities). Further, there is a risk that having contractors (versus the Agency or OIG) retrieve and provide the data stored in the cloud could affect the timeliness, integrity, and validity of the data.

We also found that none of the three contracts detailed procedures for electronic discovery (e-Discovery) when conducting a criminal investigation. While there is no evidence OIG had been affected in the past, limiting OIG access to CSP facilities and data could compromise and interfere with audits and criminal investigations, including the ability of investigators to comply with legal disclosure requirements in criminal proceedings. Additionally, without appropriate access to the CSP and related services, OIGs cannot verify that appropriate security controls are in place to manage agency risk.

[16] NIST SP 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.

[17] Federal Acquisition Regulation; FAR 52.239-1, Privacy or Security Safeguards, subpart (b) states "to the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases."

[18] The CIGIE Cloud Computing Collaboration Matrix, Question 5.7 states "Does the Cloud contract, SLA, or TOS include language allowing the Office of Inspector General full and free access to the Contractor's (and subcontractor') facilities, installations, operations, documentation, databases, and personnel used in performance of the contractor in order to conduct audits, inspections, investigations, or other reviews?"

Cloud best practices recommend that federal agencies require CSPs to allow forensic investigations for both criminal and non-criminal purposes, and that these investigations be conducted without affecting data integrity and without interference from the CSP.[19] Further, cloud best practices state that federal agencies must be able to access and retrieve electronically stored data in a cloud computing environment in a timely fashion for routine work purposes as well as litigation, discovery, and public access requests.

Recommendations: We recommend that:

1. NSF develop and implement a process that requires divisions responsible for the management of cloud services to work with the Division of Acquisition and Cooperative Support (DACS) and DIS to: (a) review cloud computing best practices, (b) develop standardized guidance for the agency to follow in acquiring cloud services, and (c) incorporate appropriate language into future contracts for cloud services. This language should permit the agency and OIG full and unrestricted access to the contractors' (and subcontractors') facilities, installations, operations, documentation, databases, and personnel used in performance of the contract in order to conduct audits, inspections, investigations, or other reviews.
2. DACS assess the feasibility of incorporating the updated contract language into existing contracts for cloud services, and if deemed feasible, do so.

Finding 3 – NSF and CSP Must Meet Federal Risk and Authorization Management Program (FedRAMP) Requirements

We found that NSF did not meet FedRAMP[20] requirements for all three of the cloud contracts reviewed. Specifically, two of the cloud contracts did not contain provisions requiring the CSP to meet and maintain FedRAMP compliance as required by OMB and FedRAMP. Although the third contract, for iTRAK, required that the cloud system be FedRAMP compliant, it had not yet achieved FedRAMP compliance when the iTRAK system became operational in October 2014, as required by OMB for all cloud services implemented on or after June 5, 2014. This occurred in part because the iTRAK cloud service providers, Accenture Federal Services (AFS) and DataPipe Government Solutions (DGS) (then Layered Tech Government Solutions), depended upon the FedRAMP schedule, process and resources to meet the FedRAMP process milestones. In addition, NSF had not implemented a process to acquire and manage cloud services that enforces all FedRAMP requirements. The NSF Office of Information and Resource Management's 2015 Information Security Handbook manual (the Handbook), suggests, but does not require use of a FedRAMP compliant CSP. Also, the Handbook's FedRAMP reference has not yet been

[19] 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. *CIGIE Cloud Computing Initiative Report*, September 2014.

[20] FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP's goal is to provide a cost-effective, risk-based approach for adopting and using cloud services. 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.

updated to require that contracts with CSPs include clauses requiring FedRAMP compliance.[21] 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. By not meeting FedRAMP contractual provision and compliance requirements, NSF does not have assurance that its information is properly protected and secured.

Specific details by CSP/contract are included in the following table:

Table: Review of NSF Contracts with CSPs for FedRAMP Requirements

	Cloud Contracts		
	AWS/DLT External SharePoint (Commercial Off-the-Shelf Licenses)	**Microsoft/ GovConnection Office 365 Email (Commercial Off-the-Shelf Licenses)**	**Accenture Federal Services iTRAK Financial Management System**
FedRAMP Compliance			
FedRAMP compliant cloud service (as of July 2015)	Yes	Yes	No
Contract has provisions/clauses requiring CSP to be FedRAMP compliant	No	No	Yes

FedRAMP was announced on December 8, 2011 via an OMB policy memorandum[22] that addressed the security authorization process for cloud computing services. Per this memorandum, beginning June 2014, federal agencies may only obtain and utilize FedRAMP-approved cloud service providers. The FedRAMP Security Assessment Framework[23] states that if a CSP obtains FedRAMP authorization, it must also perform continuous monitoring to maintain that authorization.

Additionally, OMB's December 8, 2011 policy memorandum, the FedRAMP Concept of Operations,[24] and the FedRAMP Security Assessment Framework all require federal agencies to ensure that FedRAMP requirements are met through contractual provisions. This is to ensure that a CSP has a contractual obligation to meet and maintain the FedRAMP requirements. To assist agencies in meeting this

[21] NSF's *2015 Information Security Handbook* manual, issued May 5, 2015, references the FedRAMP *Concept of Operations (CONOPS)*, Version 1.0, dated February 7, 2012. CONOPS was superseded by the *FedRAMP Security Assessment Framework* on June 6, 2014.

[22] OMB Memorandum for Chief Information Officers, *Security Authorization of Information Systems in Cloud Computing Environments*, December 8, 2011, 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.

[23] *FedRAMP Security Assessment Framework*, Version 2.0, June 6, 2014.

[24] *FedRAMP Concept of Operations*, Version 1.1, June 4, 2012.

requirement, on June 27, 2012 FedRAMP provided standard template contract language and clauses covering all FedRAMP requirements. Federal agencies can use these, or other, contract clauses during the acquisition process for cloud services to enforce FedRAMP requirements. FedRAMP-suggested contract clauses are available on www.fedramp.gov.

iTRAK, NSF's new core financial system, went live on October 14, 2014, and is a commercial off-the-shelf implementation of Oracle Federal Financials, operated on a contractor-supported cloud platform. As such, the iTRAK cloud computing system should have been authorized through the FedRAMP process by October 14, 2014. However, despite the iTRAK contract clauses requiring the CSP to be FedRAMP compliant, the iTRAK system did not meet this deadline as all cloud service layers did not achieve FedRAMP compliance in time. Moreover, iTRAK's Software as a Service (SaaS) and Platform as a Service (PaaS) layers were not FedRAMP compliant at the end of our inspection fieldwork in July 2015. The AFS SaaS layer has not yet been validated by the FedRAMP Program Management Office (GSA) nor has its completed Authority to Operate (ATO) package been posted in the secure FedRAMP repository – a key step in the FedRAMP compliance process. The DGS PaaS layer received a Joint Authorization Board (JAB) Provisional ATO[25] from FedRAMP on September 24, 2015. NSF officials stated the CSP followed all the required steps and timelines per FedRAMP's guidance and NSF has worked closely with the CSP since December 2013 to monitor iTRAK's progress through the FedRAMP approval process. NSF also stated the delay in obtaining FedRAMP compliance was because FedRAMP has a backlog, which was a main factor in GSA's process taking longer than initially anticipated.

Recommendation: We recommend that NSF develop updated guidance and implement a process to acquire and manage cloud services that enforces OMB and FedRAMP requirements. This guidance should: (a) require that cloud services utilized by NSF be FedRAMP compliant, (b) require that cloud contracts incorporate clauses requiring continued FedRAMP compliance, and (c) define the roles, responsibilities, and steps to meet and maintain FedRAMP compliance requirements.

[25] Under FISMA, the JAB cannot accept risk on behalf of any agency. Therefore, they issue 'Provisional' ATOs to indicate that a CSP has met all of the FedRAMP requirements that agencies can use to grant ATOs.

Agency Response and OIG Comments

NSF management concurs with the recommendations to strengthen NSF’s cloud computing practices.

We consider management’s comments to be responsive to our recommendations. We look forward to receiving the Corrective Action Plan and working with NSF officials to confirm implementation.

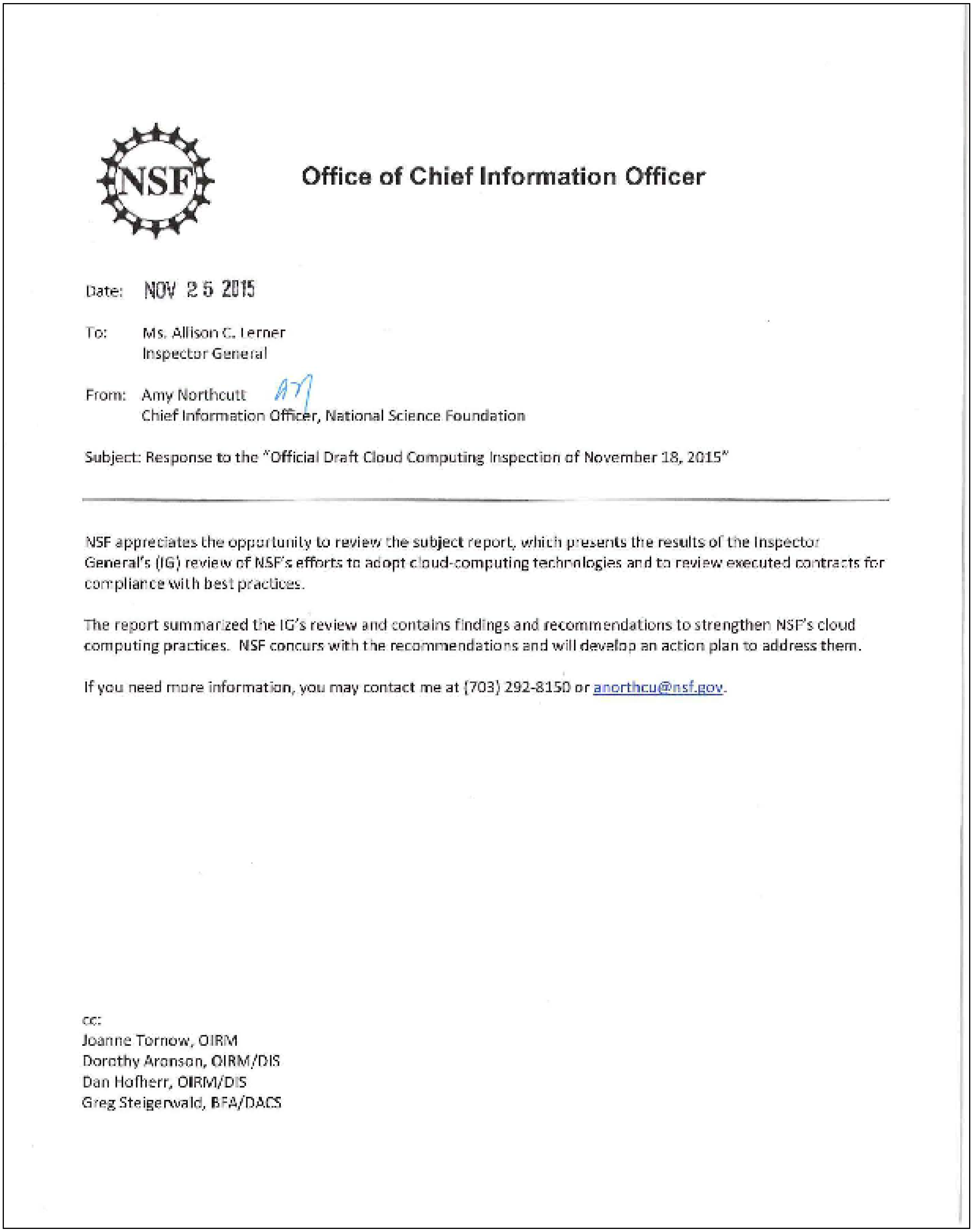
We have included NSF's response to this report in its entirety as Appendix A.

OIG Contact and Staff Acknowledgement

Thomas Moschetto – Director of Financial and IT Audits
(703) 292-7398 or tmoschet@nsf.gov

In addition to Mr. Moschetto, Emily Franko, Brian Gallagher, and Sherrye McGregor made key contributions to this report.

Appendix A: Agency Response



Office of Chief Information Officer

Date: NOV 25 2015

To: Ms. Allison C. Lerner
Inspector General

From: Amy Northcutt
Chief Information Officer, National Science Foundation

Subject: Response to the "Official Draft Cloud Computing Inspection of November 18, 2015"

NSF appreciates the opportunity to review the subject report, which presents the results of the Inspector General's (IG) review of NSF's efforts to adopt cloud-computing technologies and to review executed contracts for compliance with best practices.

The report summarized the IG's review and contains findings and recommendations to strengthen NSF's cloud computing practices. NSF concurs with the recommendations and will develop an action plan to address them.

If you need more information, you may contact me at (703) 292-8150 or anorthcu@nsf.gov.

cc:
Joanne Tornow, OIRM
Dorothy Aronson, OIRM/DIS
Dan Hofherr, OIRM/DIS
Greg Steigerwald, BFA/DACS

Appendix B: Objective, Scope, and Methodology

We performed this inspection to evaluate NSF's efforts to adopt cloud-computing technologies and to review executed contracts between the agency and cloud service providers for compliance with applicable standards. We conducted this inspection because as NSF, like the rest of the Federal Government, is increasingly utilizing cloud computing technologies, it is subjecting the agency to additional risks inherent and unique to cloud systems. With these increased vulnerabilities associated with cloud services being recognized throughout the Federal Inspector General community, we initiated this inspection as part of CIGIE's government-wide initiative to look at federal agency cloud-computing environments.

NSF reported that it had four cloud service contracts, ranging from three to five years in length, valued at approximately $27.8 million[26] as of February 25, 2015. We judgmentally selected and reviewed three of these four cloud contracts totaling approximately $27.4 million.

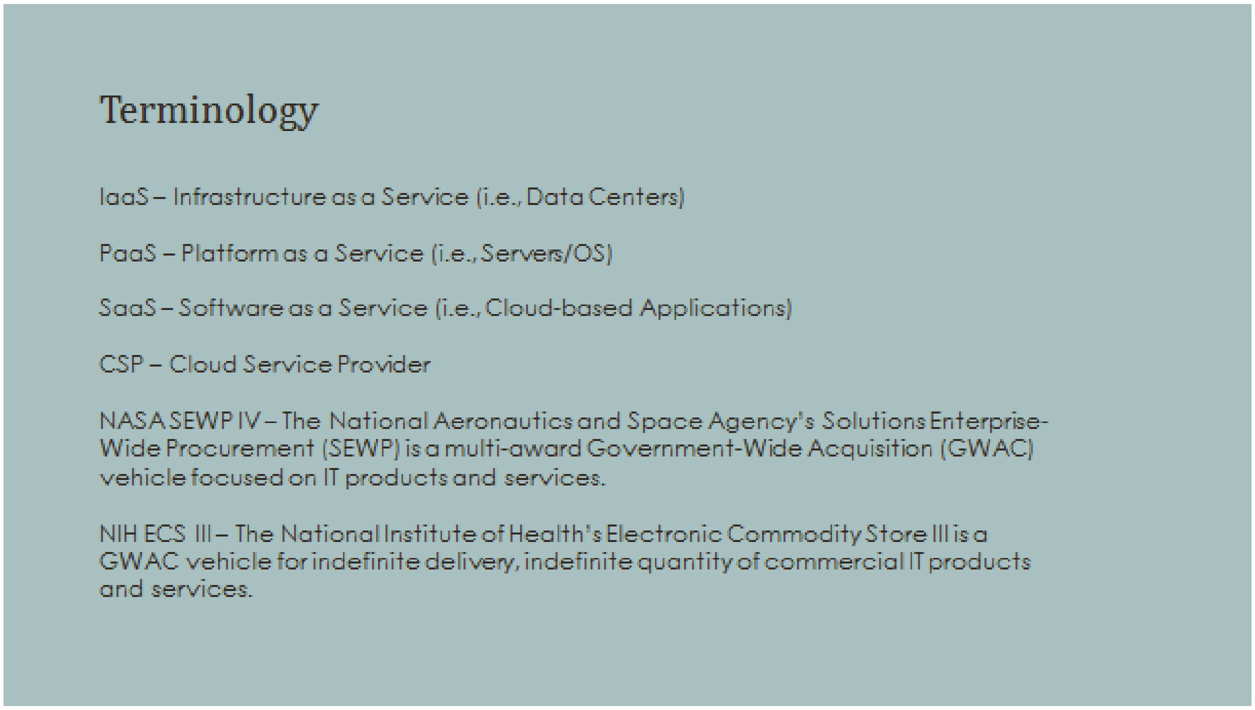
To accomplish our objectives, we reviewed contract documentation and other records pertinent to the three NSF cloud systems tested; and interviewed individuals from NSF's Division of Acquisition and Cooperative Support, Division of Information Systems, and Division of Financial Management to obtain an understanding of contract documentation and processes. We also reviewed applicable standards including laws, regulations, statutes, and cloud computing best practices and evaluated whether NSF complied with these criteria. We followed the CIGIE Cloud Computing Collaboration Matrix steps utilized by CIGIE's Cloud Computing Collaboration Initiative to complete this inspection. However, the applicability of each question in the standardized matrix of questions varied by contract. We also developed and answered additional questions (not included in the CIGIE Matrix) on whether the agency complied with best practices designed to mitigate areas deemed to be high-risk.

We conducted this inspection in accordance with Quality Standards for Inspection and Evaluation, January 2012, issued by the Council of Inspectors General on Integrity and Efficiency. These standards state that we should obtain sufficient, appropriate support to provide a reasonable basis for our findings and conclusions.

We held an exit conference with NSF management on November 12, 2015.

[26] Excluded from this figure are the three cloud service contracts NSF omitted, totaling $694,465, as discussed in the first finding of this report.

Appendix C: Contractual Relationship Diagrams



Terminology

IaaS – Infrastructure as a Service (i.e., Data Centers)

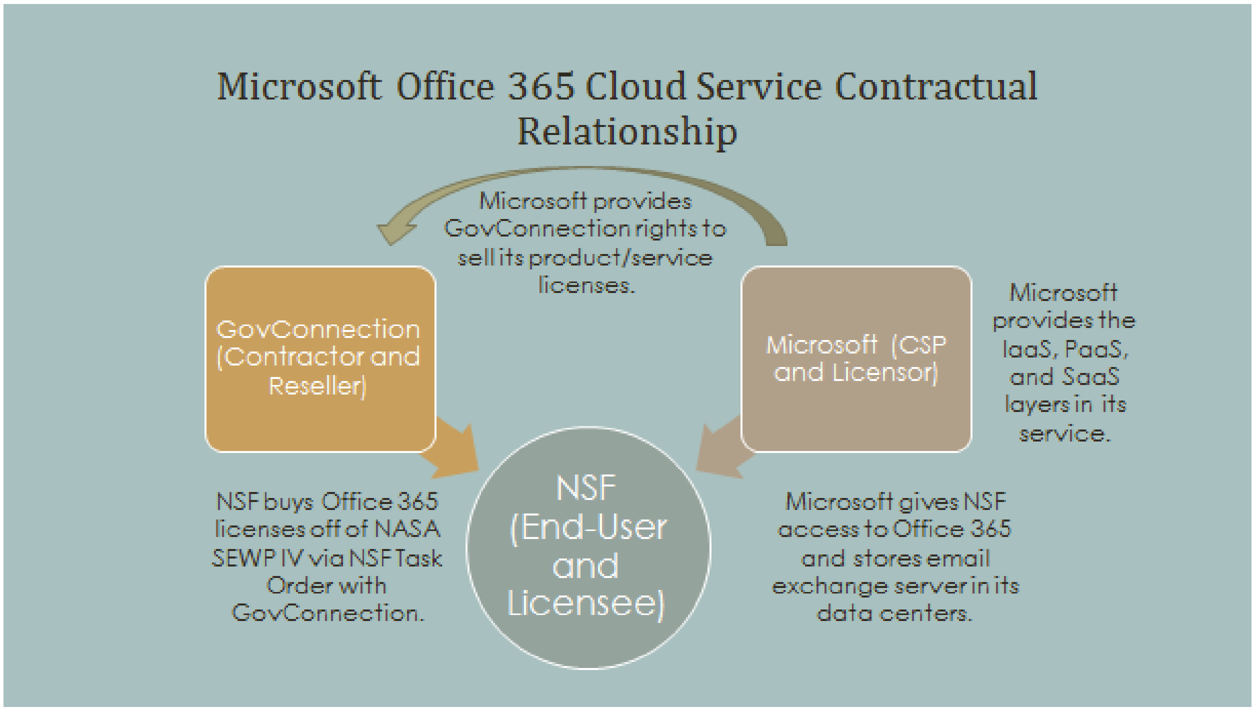
PaaS – Platform as a Service (i.e., Servers/OS)

SaaS – Software as a Service (i.e., Cloud-based Applications)

CSP – Cloud Service Provider

NASA SEWP IV – The National Aeronautics and Space Agency's Solutions Enterprise-Wide Procurement (SEWP) is a multi-award Government-Wide Acquisition (GWAC) vehicle focused on IT products and services.

NIH ECS III – The National Institute of Health's Electronic Commodity Store III is a GWAC vehicle for indefinite delivery, indefinite quantity of commercial IT products and services.



Microsoft Office 365 Cloud Service Contractual Relationship

Microsoft provides GovConnection rights to sell its product/service licenses.

GovConnection (Contractor and Reseller)

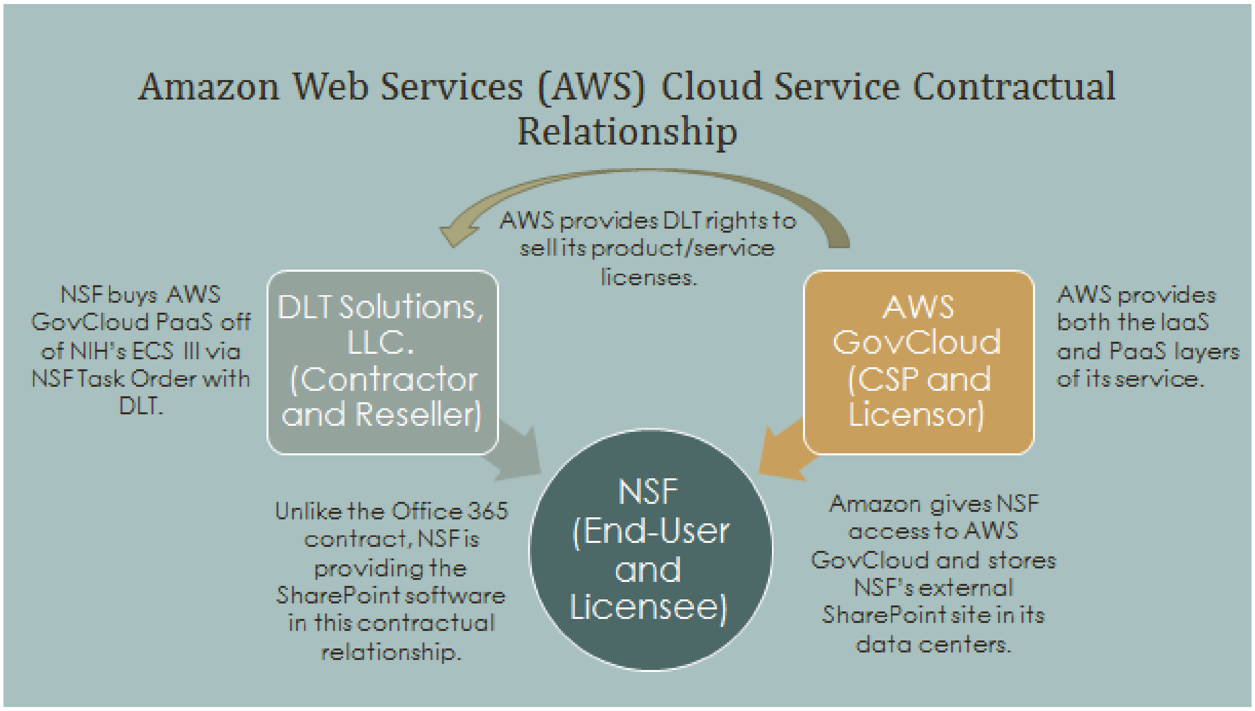
Microsoft (CSP and Licensor)

Microsoft provides the IaaS, PaaS, and SaaS layers in its service.

NSF (End-User and Licensee)

NSF buys Office 365 licenses off of NASA SEWP IV via NSF Task Order with GovConnection.

Microsoft gives NSF access to Office 365 and stores email exchange server in its data centers.



Amazon Web Services (AWS) Cloud Service Contractual Relationship

AWS provides DLT rights to sell its product/service licenses.

NSF buys AWS GovCloud PaaS off of NIH's ECS III via NSF Task Order with DLT.

DLT Solutions, LLC. (Contractor and Reseller)

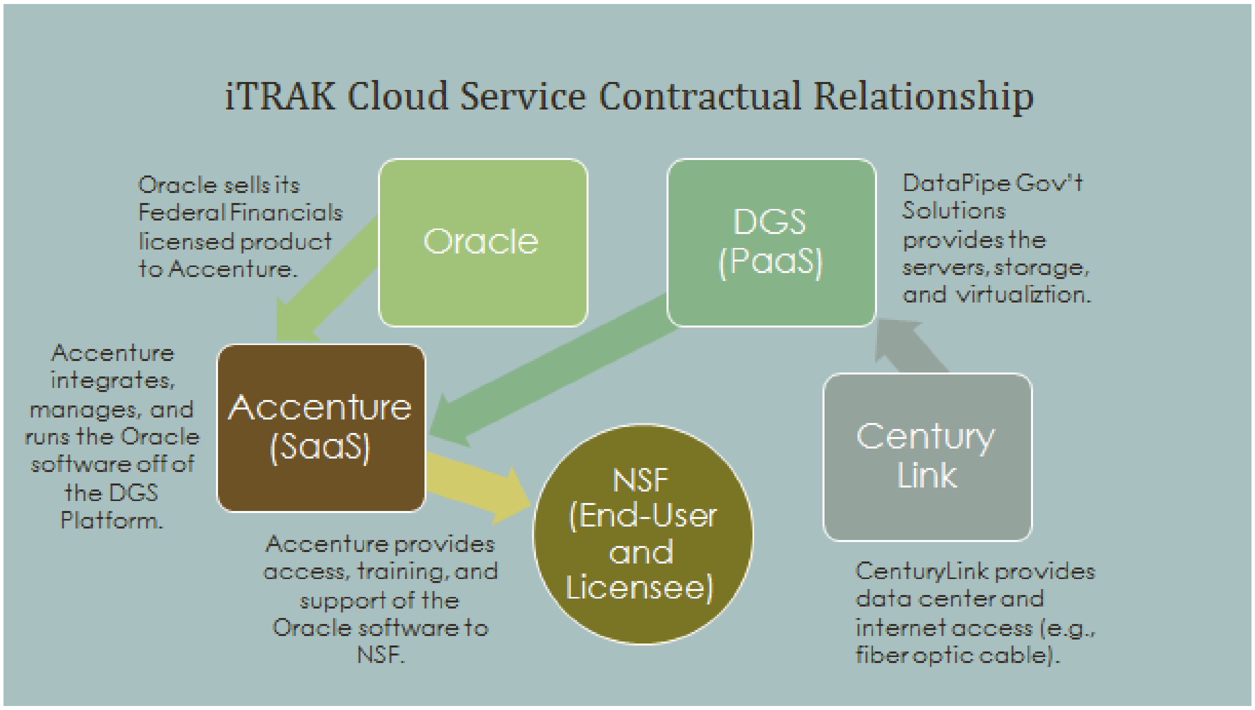
AWS GovCloud (CSP and Licensor)

AWS provides both the IaaS and PaaS layers of its service.

NSF (End-User and Licensee)

Unlike the Office 365 contract, NSF is providing the SharePoint software in this contractual relationship.

Amazon gives NSF access to AWS GovCloud and stores NSF's external SharePoint site in its data centers.



iTRAK Cloud Service Contractual Relationship

Oracle sells its Federal Financials licensed product to Accenture.

Oracle

DGS (PaaS)

DataPipe Gov't Solutions provides the servers, storage, and virtualiztion.

Accenture integrates, manages, and runs the Oracle software off of the DGS Platform.

Accenture (SaaS)

NSF (End-User and Licensee)

Century Link

Accenture provides access, training, and support of the Oracle software to NSF.

CenturyLink provides data center and internet access (e.g., fiber optic cable).