



**OFFICE OF
INSPECTOR GENERAL**
UNITED STATES POSTAL SERVICE

**Cloud
Computing
Contract
Clauses**

**Management
Advisory Report**

Report Number
SM-MA-14-005-DR

April 30, 2014



OFFICE OF INSPECTOR GENERAL

UNITED STATES POSTAL SERVICE

Highlights

The 13 cloud computing contracts did not address information accessibility and data security for network access and server locations because the *Information Security* handbook in effect at the time of the contract award did not include these requirements.

Background

Cloud computing uses remote servers on the Internet to manage, store, and process data. Using cloud computing reduces costs while increasing the efficiency of services; however, it also has risks associated with data leaks and loss of public trust. U.S. Postal Service Supply Management (Technology Infrastructure Portfolio) contracting officials awarded 13 contracts totaling about \$303 million for cloud computing services from fiscal years 2007 to 2013. The Postal Service's *Information Security* handbook of 2002 was in effect when officials awarded these contracts.

The Council of Inspectors General on Integrity and Efficiency issued a memorandum in 2011 on information accessibility, data security, and privacy concerns that federal agencies should consider before entering into cloud computing contracts. The memorandum identifies areas of concern for federal agencies but is not mandatory for the Postal Service. In August 2013, the Postal Service issued the *Cloud Security* handbook establishing information security policies and requirements to protect its information in a cloud computing environment.

Our objective was to assess whether cloud computing contracts have adequate controls to address information accessibility, data security, and privacy concerns.

What The OIG Found

The 13 cloud computing contracts did not address information accessibility and data security for network access and server locations because the *Information Security* handbook in effect at the time of the contract award did not include these requirements. In addition, the Postal Service exempted a supplier from following the handbook for one contract that did not contain sensitive data. Although the data may not be sensitive, the handbook provides additional requirements such as insurance against losses resulting from data breaches and procedures for timely notification of these breaches.

The Postal Service's *Cloud Security* handbook addresses the information accessibility and data security gaps. However, contracting officials were concerned that including the policy in existing cloud computing contracts could increase contract costs. As a result, we identified potential costs of \$12,429,228 for mitigating cloud security risks.

What The OIG Recommended

We recommended management include *Information Security* and *Cloud Security* handbook requirements in future cloud computing contracts, regardless of data sensitivity, and assess the costs and benefits of incorporating these requirements into existing cloud computing contracts.

Transmittal Letter

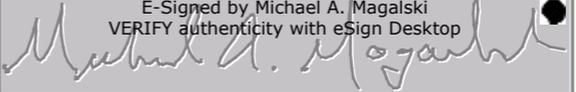


OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

April 30, 2014

MEMORANDUM FOR: SUSAN BROWNELL
VICE PRESIDENT, SUPPLY MANAGEMENT

CHARLES L. MCGANN
MANAGER, CORPORATE INFORMATION SECURITY

E-Signed by Michael A. Magalski
VERIFY authenticity with eSign Desktop


FROM: Michael A. Magalski
Deputy Assistant Inspector General
for Support Operations

SUBJECT: Management Advisory Report – Cloud Computing Contract
Clauses (Report Number SM-MA-14-005)

This report presents the results of our review of Cloud Computing Contract Clauses (Project Number 13YG033SM000).

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Monique P. Colter, director, Supply Management and Facilities, or me at 703-248-2100.

Attachment

cc: Corporate Audit and Response Management

Table of Contents

Cover	
Highlights.....	1
Background.....	1
What The OIG Found.....	1
What The OIG Recommended	1
Transmittal Letter.....	2
Findings	4
Introduction	4
Conclusion	4
Cloud Computing Contracts and Policy	4
Information Accessibility.....	5
Data Security.....	5
Recommendations.....	8
Management’s Comments	8
Evaluation of Management’s Comments	8
Appendices.....	9
Appendix A: Additional Information	10
Background	10
Objective, Scope, and Methodology.....	10
Prior Audit Coverage	11
Appendix B: Other Impact.....	12
Appendix C: Management’s Comments	13
Contact Information	15

Findings

The 13 cloud computing contracts did not address information accessibility and data security for network access and server locations.

Contract language that inadequately addresses information accessibility and data security concerns increase the risk of data compromises and system breaches. As a result, we identified potential costs of \$12,429,228 for mitigating cloud security risks.

Introduction

This report presents the results of our review of Cloud Computing Contract Clauses (Project Number 13YG033SM000). Our objective was to assess whether U.S. Postal Service cloud computing contracts have adequate controls to address information accessibility, data security, and privacy concerns. See [Appendix A](#) for additional information about this review.

Cloud computing uses remote servers on the Internet to manage, store, and process data. Using cloud computing reduces costs while increasing the efficiency of services; however, it also has risks associated with leakage of data and loss of public trust. Postal Service Supply Management Technology Infrastructure Portfolio¹ contracting officials awarded 13 contracts totaling about \$303 million for cloud computing services from fiscal years (FY) 2007 to 2013. The Postal Service *Information Security* handbook² of 2002 was in effect when officials awarded these contracts.

The Council of Inspectors General on Integrity and Efficiency (CIGIE)³ issued a memorandum in 2011 on the information accessibility, data security, and privacy concerns federal agencies should consider before entering into cloud computing contracts. The memorandum identifies areas of concern for federal agencies but is not mandatory for the Postal Service. In August 2013, the Postal Service issued policies⁴ that established information security procedures and requirements to protect its information in a cloud computing environment.

Conclusion

The 13 cloud computing contracts did not address information accessibility and data security for network access and server locations. The version of Handbook AS-805 that was in effect when officials awarded the contracts did not include these as requirements. In addition, the Postal Service exempted a supplier from following the handbook in one contract because the contract did not contain sensitive data. Although data may not be sensitive, Handbook AS-805 provides additional requirements for insurance against losses resulting from data breaches and making timely notification of these breaches. Handbook AS-805H addressed the information accessibility and data security gaps; however, contracting officials were concerned that including the policy in existing cloud computing contracts could increase contract costs.

Contract language that inadequately addresses information accessibility and data security concerns increase the risk of data compromises and system breaches. As a result, we identified potential costs of \$12,429,228 for mitigating cloud security risks. See [Appendix B](#) for additional information on other impact.

Cloud Computing Contracts and Policy

The Postal Service included language in 13 cloud computing contracts to address privacy concerns; however, it did not include adequate language to address information accessibility and data security for network access and server locations. The information security policy in effect at that time did not include these requirements. In August 2013, the Postal Service updated Handbook AS-805H to bridge gaps in the information security policy.

-
- 1 The Technology Infrastructure Portfolio is responsible for managing the purchase of technology-related products and services, such as retail systems, telecommunications, and information technology (IT) hardware and software.
 - 2 Handbook AS-805, *Information Security*, 2002.
 - 3 The CIGIE develops policies, standards, and approaches to aid in the establishment and training of the Offices of Inspectors General.
 - 4 Handbook AS-805H, *Cloud Security*, August 2013.

Information Accessibility

The Postal Service did not require Cloud Service Providers (CSP) for all 13 contracts to state the amount of access they should have to the network over which postal information and data travel. The Postal Service did not require real-time monitoring capability and network access for the U.S. Postal Service Office of Inspector General (OIG) in one contract. The Postal Service should maintain access to the network to perform tests and ensure necessary access is available to security officials for investigative functions. It should also have real-time monitoring capability to guard against external attacks. OIG access is equally important when addressing information accessibility concerns. *Supplying Principles and Practices (SP&P)*⁵ gives the Postal Service access to the CSP records; however, it does not specifically address OIG access to the cloud network to audit and investigate programs and employees.

Data Security

The Postal Service did not require CSPs for all 13 contracts to provide the locations of all servers containing Postal Service data. In addition, the Postal Service did not include language to address the following in one contract:

- **Incident Responsiveness** – This ensures the vendor is aware of Postal Service requirements for mitigation and notification of data breaches and loss. The Postal Service should be aware of server locations and know where information is stored for accountability.
- **Restricted Access** – Restricting access to the servers and cloud data ensures that only authorized individuals have access.
- **Vendor Indemnification** – Vendors should indemnify⁶ the Postal Service from accepting responsibility for the costs and liability of data breaches and loss.
- **Cloud Data Ownership** – Although vendors may be responsible for the cloud environment, the data belong to the Postal Service and contract language must specify ownership and requirements for disposal of cloud data after contract completion.

The CIGIE issued a memorandum⁷ in 2011 identifying potential concerns that federal agencies should consider before entering into cloud computing contracts. These concerns are in the areas of data security, information accessibility, and regulatory compliance. The memorandum identified sub-areas within the three major areas of concern.⁸ Addressing these concerns would help prevent system breaches and data leaks and ensure access to information needed for investigations (see [Table 1](#)).

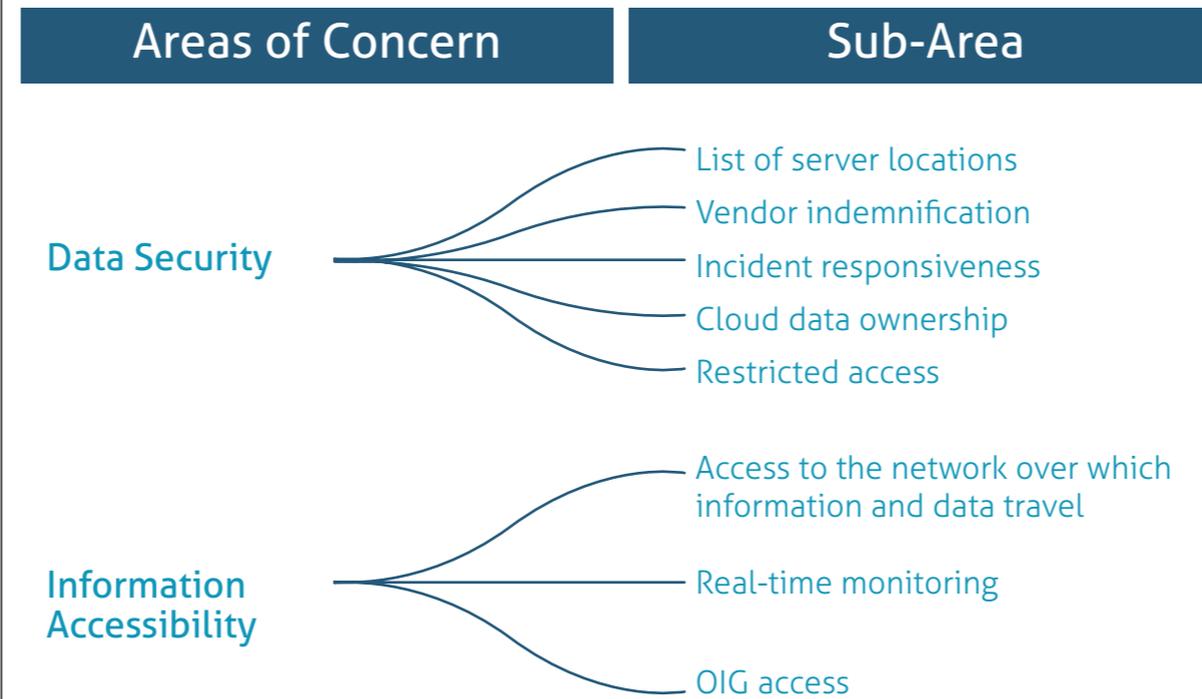
⁵ SP&P Clause 4-2, Contract Terms and Conditions Required to Implement Policies, Statutes or Executive Orders (July 2009).

⁶ Indemnification protects the Postal Service by requiring CSPs to pay for possible future damage or loss.

⁷ *Cloud Computing Contracting Concerns*, 2011.

⁸ The CIGIE memorandum listed eight major areas of concern. Our scope examined three major areas of concern because the remaining concerns overlapped topics addressed in those three areas or were addressed in the SP&P.

Table 1. Cloud Computing Contract Concerns



Contracts at risk
Contract value

Hover over boxes to see which area of concern affects the contracts at risk.

Sources: CIGIE memorandum and OIG analysis.

At the time the Postal Service awarded¹⁰ the 13 contracts, it had an information security policy that addressed seven of the nine topics within the three major areas of concern we reviewed. However, the policy did not address access to the network over which Postal Service information and data travel or cloud server locations. Contracting officials did not include the information security policy or SP&P Clause 4-19, Information Security, which references these policies,¹¹ and other information security-related handbooks in the contract language for one of the 13 contracts. Officials obtained a waiver from the Corporate Information Security Office (CISO)¹² excluding this contract from the provisions of Clause 4-19 because the contract did not contain sensitive information. Although the data may not have been considered sensitive, Clause 4-19 provides additional protections and should be in all IT contracts. Further, the CSP is a [REDACTED]. Although the CISO approved a waiver excluding the clause, the Postal Service was still exposed to increased data security and information accessibility risks as the data were housed outside the country. Postal Service policy requires all servers, including back-up servers, to be in the contiguous U.S.¹³

9 One contract did not include Handbook AS-805, *Information Security*, requirements and did not address cloud computing concerns 3 through 9, as depicted in Table 1.
 10 The Postal Service awarded the 13 contracts from FYs 2007 to 2013.
 11 Handbook AS-805 establishes policies to appropriately identify, classify, and protect Postal Service information resources.
 12 CISO establishes the overall strategic and operational plan for Postal Service information security programs and necessary implementation strategies.
 13 AS-805H Section 8-3, *Privacy Contract Requirements*, states that data stored outside the U.S. cannot be protected under the Privacy Act and may allow for certain local or foreign law enforcement authorities to search Postal Service data pursuant to a court order, subpoena, or informal request outside the control of the Postal Service.

In August 2013, the Postal Service issued Handbook AS-805H, which bridged gaps in the information security policy and incorporated Federal Risk and Authorization Management Program (FedRAMP)¹⁴ certification requirements. It requires CSPs to provide the Postal Service with their server locations and state the amount of access to the network the Postal Service should retain. However, contracting officials stated they did not plan to modify SP&P Clause 4-19 to include the requirements of the new cloud security policy because they did not have guidance on cloud computing and did not receive a request from the CISO to update the SP&P. Contracting officials also stated they did not plan to modify existing contracts to include the increased security requirements, such as compliance with FedRAMP, because it may require CSPs to change their business processes or systems and would increase contract costs.

Two of the CSPs,¹⁵ whose three contracts totaled \$136,114,238, are FedRAMP-certified; therefore, the Postal Service should not be subject to additional costs for incorporating FedRAMP into the contracts. In addition, [REDACTED] a CSP to whom the Postal Service awarded a contract valued at \$2 million in August 2013, voluntarily proposed pursuing FedRAMP certification in its technical proposal, although it was optional in the solicitation.

The Postal Service's issuance of Handbook AS-805H shows that it is aware of the significant risks in using cloud computing services; however, without guidance on procuring cloud computing contracts and contractual language requiring CSPs to comply with the new cloud security policy, the Postal Service remains exposed to potential information accessibility and data security risks in the cloud computing environment.

The Ponemon Institute, which conducts independent research on privacy, data protection, and information security, issued a study on the cost of cyber crime.¹⁶ The study indicates that information theft, including theft of trade secrets and customer information, is the most critical consequence of a cyber attack. The loss of customer information could have an adverse effect on the goodwill of and impact on the Postal Service brand. Additionally, the Ponemon study indicated the average cost to resolve a cyber attack is \$1,035,769 per incident. Based on this information, we estimate the Postal Service's potential exposure costs associated with 12¹⁷ contracts could be as high as \$12,429,228 (see [Appendix B](#)).

¹⁴ A government-wide program established in December 2011 that standardizes how federal agencies incorporate security assessment, authorization, and continuous monitoring for cloud computing contracts. Although exempt from the program, the Postal Service chooses to comply.

¹⁵ [REDACTED]

¹⁶ Ponemon Institute *2013 Cost of Cyber Crime: United States*, October 2013.

¹⁷ We excluded one contract from our calculation because it had expired.

Recommendations

We recommend management include requirements from Handbook AS-805, *Information Security*, and Handbook AS-805H, *Cloud Security*, in future cloud computing contracts regardless of data sensitivity.

We recommend the vice president, Supply Management, in coordination with the manager, Corporate Information Security:

1. Include requirements from Handbook AS-805, *Information Security*, and Handbook AS-805H, *Cloud Security*, in future cloud computing contracts regardless of data sensitivity.

We recommend the vice president, Supply Management:

2. Assess the cost and benefits of negotiating post-award agreements with cloud service providers to incorporate requirements from Handbook AS-805, *Information Security*, and Handbook AS-805H, *Cloud Security*, into existing cloud computing contracts.

Management's Comments

Management generally agreed with the finding, recommendations, and other impact associated with this report.

In response to recommendation 1, management stated they have directed the IT Software, Services and Retail Systems and Telecom and Information Hardware Category Management Centers to include Handbooks AS-805 and AS-805H in all new cloud-based contracts. However, Supply Management, in coordination with the CISO, will issue guidance to all contracting officials and others in the Chief Information Officer's office on incorporating the referenced handbooks; using appropriate clauses; and summarizing the necessity for information accessibility, data security for network access, and capturing server location details in future cloud computing contracts. The target implementation date is June 2014.

Regarding recommendation 2, management will obtain the pricing impact of modifying the 13 contracts identified in this report to include Handbooks AS-805 and AS-805H requirements. Contracting officials and the requirements office will assess the associated costs to determine whether the benefits of including the handbooks' requirements in the contract outweigh the additional cost. The target implementation date is July 2014.

See [Appendix C](#) for management's comments, in their entirety.

Evaluation of Management's Comments

The OIG considers management's comments responsive to the recommendations and corrective actions should resolve the issues identified in the report. The OIG considers all the recommendations significant, and therefore requires OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. These recommendations should not be closed in the Postal Service's follow-up tracking system until the OIG provides written confirmation that the recommendations can be closed.

Appendices

*Click on the appendix title
to the right to navigate to
the section content.*

Appendices.....	9
Appendix A: Additional Information	10
Background	10
Objective, Scope, and Methodology.....	10
Prior Audit Coverage	11
Appendix B: Other Impact.....	12
Appendix C: Management’s Comments	13

Appendix A: Additional Information

Background

Cloud computing is the practice of using remote servers on the Internet to manage, store, and process data. The Postal Service Supply Management Technology Infrastructure Portfolio's contracting officials awarded 13 contracts totaling about \$303 million for cloud computing services from FYs 2007 to 2013.

The CIGIE issued a memorandum in 2011 outlining the concerns that federal agencies must be aware of before entering into cloud computing contracts. The memorandum identified eight areas of concern – information accessibility, data security, regulatory compliance, termination and transition, asset availability, maintenance, pricing and time, and intellectual property. Our review focused on three areas – information accessibility, data security, and regulatory compliance related to privacy.

FedRAMP supplements the National Institute of Standards and Technology's¹⁸ (NIST) *Special Publications*, which provide federal agencies with a information systems risk management framework. Several agencies, including the U.S. Department of Homeland Security, U.S. Department of Defense, and U.S. General Services Administration, coordinated the development of FedRAMP. In December 2011, before the establishment of FedRAMP, each agency developed and incorporated cloud security measures into its own contract. Severe overlap and inefficiency existed because each agency managed its own security risks and provided security assessments and authorizations for each IT system used. This was costly and inefficient as agencies may have assessed, authorized, and deployed the same system. FedRAMP security protocols provide one-stop shopping for federal agencies and CSP with a process that is completed once but used many times.

Objective, Scope, and Methodology

Our objective was to assess whether the Postal Service's cloud computing contracts have adequate controls to address information accessibility, data security, and privacy concerns. Our scope was limited to 13 cloud computing contracts identified by the Supply Management Technology Infrastructure Portfolio that were awarded between FYs 2007 and 2013. To accomplish our objective, we:

- Reviewed Postal Service policies, procedures, and guidelines related to audits, investigations, and privacy.
- Reviewed federal government laws and regulations.
- Reviewed the CIGIE IT Subcommittee memorandum on cloud computing contracting concerns.
- Reviewed the CIGIE IT Subcommittee's proposed *Federal Acquisition Regulation* clause addendum.
- Reviewed documentation for 13 cloud computing contracts to determine whether Postal Service contracting officials:
 - Solicited contracts with FedRAMP requirements.
 - Included security requirements that protect the Postal Service cloud contracts.
 - Included language in cloud computing contracts allowing equal accessibility requirements for the OIG.

¹⁸ NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all federal agencies.

- Interviewed OIG Office of General Counsel and IT staff to learn about the applicability of FedRAMP requirements to the Postal Service.

We conducted this review from August 2013 through April 2014, in accordance with the CIGIE, *Quality Standards for Inspection and Evaluation*. We discussed our observations and conclusions with management on April 7, 2014, and included their comments where appropriate.

We assessed the reliability of computer-generated data by comparing the contract values obtained from the Postal Service's Enterprise Data Warehouse to hard copy contract documentation. We determined that the data were sufficiently reliable for the purposes of this report.

Prior Audit Coverage

The OIG issued *Cloud Computing* (Report Number IT-AR-12-006, dated May 9, 2012), which concluded that opportunities exist for the Postal Service to use cloud computing technology to support IT operations, resources, and infrastructure. However, no overarching adoption strategies exist to determine which cloud deployment or service models are best suited for current IT operations or resources. The Postal Service did not have a consistent strategy or approach for determining the risks and benefits of implementing cloud computing technology. The OIG made three recommendations, including development of a common definition for cloud computing technology within the Postal Service and a cloud computing technology strategy. Management agreed with the findings and recommendations.

Appendix B: Other Impact

Recommendation	Impact Category	Amount
1	IT Security ¹⁹	\$12,429,228

We calculated other impact based on 12 potential applications at risk²⁰ and the Ponemon Institute's 2013 research report,²¹ which revealed the average cost per breach to an organization (\$1,035,769). Each contract represents a separate Postal Service application. We derived the total other impact by multiplying \$1,035,769 by 12 (the number of applications at risk) because the active contracts did not include adequate contract language to address information accessibility and data security concerns.

¹⁹ IT security includes computer software, networks, and data that are vulnerable or at risk of loss because of fraud, inappropriate or unauthorized disclosure of sensitive data, or disruption of critical Postal Service operations and services.

²⁰ The Supply Management Technology Infrastructure Portfolio manager provided a list of 13 cloud computing contracts in September 2013. We excluded one contract from our calculation because it had expired.

²¹ Ponemon Institute, *2013 Cost of Cyber Crime: United States*, October 2013.

Appendix C: Management's Comments



April 24, 2014

JUDITH LEONHARDT

SUBJECT: Response to Draft Management Advisory Report – Cloud Computing Contract Clauses (Report Number SM-MA-14-DRAFT)

Thank you for providing the Postal Service with the opportunity to review and comment on the subject draft report. Management is in general agreement with the Office of Inspector General's (OIG) findings, recommendations and monetary impact associated with the Cloud Computing Contract Clauses Audit.

OIG Audit Recommendations:

We recommend the vice president, Supply Management, in coordination with the manager, Corporate Information Security:

Recommendation 1: Include Handbook AS-805, *Information Security*, and Handbook AS-805-H, *Cloud Security* requirements in future cloud computing contracts regardless of data sensitivity.

Management Response: Management agrees with this recommendation. The IT Software, Services and the Retail Systems Category Management Center (CMC) and Telecom & Information Hardware CMC have been under direction to include Handbooks AS-805 and AS-805-H in all new cloud based contracts. However, Supply Management in coordination with the Manager, Corporate Information Security, will issue a communication to all contracting officials and others within the Chief Information Officer's organization. This communication will provide notification and guidance for incorporating the referenced Handbooks, use of appropriate clauses, and summarizing the necessity for information accessibility, data security for network access, and capturing server locations details into future cloud computing contracts.

Target Implementation Date: June 2014

Responsible Manager: Manager, Technology Infrastructure Portfolio, Supply Management and Manager, Corporate Information Security.

We recommend the vice president, Supply Management:

Recommendation 2: Assess the cost and benefits of negotiating post-award agreements with cloud service providers to incorporate Handbook AS-805, *Information Security*, and Handbook AS-805-H, *Cloud Security*, in existing cloud computing contracts.

Management Response: Management agrees with this recommendation and will obtain the pricing impact of modifying the 13 in-scope contract suppliers identified in this report to incorporate Handbooks AS-805, as necessary, and AS-805-H requirements into their contracts. Any associated costs will be assessed by contracting officials and the requirements office to determine if the benefits outweigh the additional costs of any equitable adjustments.

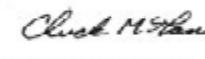
Target Implementation Date: July 2014.

Responsible Manager: Manager, Technology Infrastructure Portfolio, Supply Management and Manager, Corporate Information Security.

This report and management's response does not contain proprietary or sensitive business information that may be exempt from disclosure pursuant to the Freedom of Information Act. If you have any questions about this response, please contact Susan Witt at (202) 268-4833.



Susan M. Brownell
Vice President, Supply Management



2014.04.24
14:57:05 -04'00'

Charles McGann
Manager, Corporate Information Security

cc: Corporate Audit Response Management



Contact us via our [Hotline](#) and [FOIA](#) forms, follow us on social networks, or call our Hotline at 1-888-877-7644 to report fraud, waste or abuse. Stay informed.

1735 North Lynn Street
Arlington, VA 22209-2020
(703) 248-2100