OFFICE OF
INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

U.S. Postal Service Data Governance

Audit Report

April 23, 2013

OFFICE OF INSPECTOR GENERAL

UNITED STATES POSTAL SERVICE

HIGHLIGHTS

April 23, 2013

**U.S. Postal Service
Data Governance**

Report Number DP-AR-13-004(R)

BACKGROUND:

The U.S. Postal Service operates one of the largest information technology infrastructures in the world and has an inventory of 795 computer applications. Data from many of those applications are collected into data repositories and shared widely within the Postal Service. Using those assets to make informed decisions is particularly important for the Postal Service, as declining revenue, the struggling national economy, and the increasingly digital nature of the world threaten its core business. One of its key strategies is to leverage its strengths by integrating data to improve business decisions.

In fiscal year (FY) 2012, the U.S. Postal Service Office of Inspector General (OIG) conducted a series of audits related to how the Postal Service uses data to manage its operations. We also examined data governance, the process to ensure that data are managed and fully utilized, in six best-in class companies to identify best practices that the Postal Service might adopt to optimize resources and efforts.

Our objective was to determine whether the Postal Service was effectively managing and using data in a manner that assists employees in achieving strategic and operational goals.

WHAT THE OIG FOUND:

The Postal Service could improve management of critical data to assist managers and employees to achieve strategic and operational goals. We identified 148 data-related issues in OIG reports issued in FYs 2009 through 2012. The majority of the issues involved unreliable or inaccurate data or were caused by an absence of policies or the Postal Service not enforcing existing policies.

Although the Postal Service defined a structure for a data governance program in 2003, full roles and responsibilities were not uniformly adopted across the enterprise. Also, limitations in the Postal Service's data governance program placed the Postal Service at risk to potential vulnerabilities that could affect data quality, availability, and integrity and result in inefficient operations, disruptions of service, and fraud.

We identified best practices used by companies with successful data governance programs. We used these best practices to identify a possible implementation strategy.
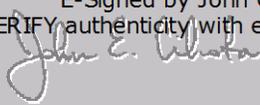
WHAT THE OIG RECOMMENDED:

We recommended implementing a formal, enterprise-wide data governance program.

Link to review the entire report

April 23, 2013

MEMORANDUM FOR: ELLIS A. BURGOYNE
CHIEF INFORMATION OFFICER AND EXECUTIVE VICE
PRESIDENT

E-Signed by John Cihota
VERIFY authenticity with eSign Deskto

John E. Cihota

FROM: John E. Cihota
Deputy Assistant Inspector General
for Financial and Systems Accountability

SUBJECT: Audit Report – U.S. Postal Service Data Governance
(Report Number DP-AR-13-004(R))

This report presents the results of our audit of U.S. Postal Service Data Governance
(Project Number 12BG007FF000).

We appreciate the cooperation and courtesies provided by your staff. If you have any
questions or need additional information, please contact Kevin H. Ellenberger, director,
Data Analysis and Performance, or me at 703-248-2100.

Attachments

cc: James P. Cochrane
John T. Edgar
Corporate Audit and Response Management

TABLE OF CONTENTS

Introduction

This report presents the results of our audit of U.S. Postal Service Data Governance (Project Number 12BG007FF000). For fiscal year (FY) 2012, the U.S. Postal Service Office of Inspector General (OIG) conducted a series of audits related to how the Postal Service uses data to manage its operations. This capping report focuses upon the data governance issues we found in those audits and other OIG audits conducted over the last 4 years as well as additional analysis conducted. Our objective was to determine whether the Postal Service was effectively managing and using data in a manner that assists employees in achieving strategic and operational goals. This self-initiated audit addresses strategic risk. See Appendix A for additional information about this audit.

The Postal Service operates one of the largest information technology (IT) infrastructures in the world and has an inventory of 795 computer applications. Data from many of those applications is collected into data stores and shared widely within the Postal Service. Using those assets to make informed decisions is particularly important for the Postal Service, as declining revenue, the struggling national economy, and the increasingly digital nature of the world threaten its core business. Organizations initiate data governance programs to strategically address issues similar to those faced by the Postal Service.

Data governance is the management process ensuring important data assets are formally managed and fully utilized throughout the organization. A 2008 survey[1] revealed three primary factors that provide the impetus for data governance initiatives: risk mitigation, revenue optimization, and cost control. Additionally, recent industry studies on the cost of poor data governance estimate that organizations, on average, spend $5-$8.2 million annually due to data quality issues. This cost is driven primarily by the loss of end-user productivity that results from poorly organized, low quality, and inaccessible data, and bad business decisions based on that data.

Conclusion

The Postal Service could improve management of critical data to assist managers and employees in achieving strategic and operational goals. We reviewed and analyzed OIG reports issued in FYs 2009 through 2012 and identified limitations in the Postal Service's data governance program, which include:

- Inconsistent corporate-wide data strategy.
- Unreliable and inaccurate data.
- Data inconsistencies within the Enterprise Data Warehouse (EDW).[2]

---

[1] *Information Age* magazine surveyed 279 organizations.
[2] EDW is a central, enterprise-wide database that contains information extracted from operational systems. Data governance initiatives look to organize and centralize data warehouses to ensure data are stored correctly.

- Insufficient IT security measures.
- Difficulties with accessing and sharing data.

Although the Postal Service defined a framework for a data governance program in a 2003 management instruction,[3] full roles and responsibilities were not uniformly adopted across all enterprise business units. In addition, the Postal Service did not create formalized enterprise-wide data governance programs with structures, policies, and processes to govern data storage and use. Because of limitations in the Postal Service's data governance program, the Postal Service risks potential vulnerabilities that could hamper the quality, availability, and integrity of the organization's data and result in inefficient operations, disruptions of service, and potential fraud.

Our report outlines 34 industry data governance best practices the Postal Service should consider to foster and institutionalize a strong culture and capability for a data governance program.

Limitations in the Postal Service's Data Governance Program

Currently, the Postal Service does not have a comprehensive, centralized data governance program that better allows it to provide quality data that can be easily or instantly accessed, essential to ensuring that managers can accomplish their goals, further reduce costs, and improve decision making. For example, improved data quality and availability will enable business users to more effectively analyze corporate data to identify opportunities for cost savings and new revenue streams.

The Postal Service defined a program for a data governance program in its 2003 Management Instruction AS-860-2003-2. The guidance included roles and responsibilities for the data stewards, portfolio managers, and business area executive sponsors. However, full roles and responsibilities were not uniformly adopted across the Postal Service's business units. For example, IT management require business areas to select a data steward if they store data in the EDW. However, data stewards are not in place to support the integrity of other critical data assets under the control of the business areas, as required. Therefore, the Postal Service lacks consistent enterprise -wide data management policies and organizational structures to supervise data governance across different functional areas.

The Postal Service is committed to providing an IT infrastructure that supports customer, corporate, and business needs. As stated in *Vision 2013*,[4] one of the Postal Service's key strategies is to leverage its strengths by integrating data to improve business decisions. In doing so, the Postal Service must update data systems and provide a centralized data governance program to standardize reporting and eliminate duplicate processes. Additionally, one of the Deliver Results, Innovation, Value, and

---

[3] Management Instruction AS-860-2003-2, *Data Stewardship: Data Sharing Roles and Responsibilities*, dated March 6, 2003.
[4] *Vision 2013, Five-Year Strategic Plan for 2009-2013*, October 2008.

Efficiency (DRIVE) strategic priorities[5] is enabling and empowering systems that aim to position the Postal Service for future success.

During our audit, we reviewed and analyzed OIG reports issued during FYs 2009 through 2012 and identified 148 data-related issues. These past reports identified significant measurable benefits that could be realized if data were better managed. We categorized those findings within the five component areas of data governance.

Inconsistent Corporate-Wide Data Strategy

Corporate-wide data strategy describes the strategic approach to establishing and maintaining a data governance program. Successful data governance programs require clear delineation of roles and responsibilities of corporate stakeholders, a visible and active leadership structure, and a defined strategic plan. During our review of OIG reports, we noted conditions related to corporate-wide data strategy that may have been prevented by a strengthened data governance program. For example:

- The Postal Service did not have a consistent strategy or approach for determining the risks and benefits of implementing cloud computing technology.[6] Having a consistent strategy and approach to cloud computing technology would allow management to develop an optimal cloud computing model to increase business and operating efficiency and lower infrastructure cost. We estimated an annual potential cost savings of $2.6 million using cloud computing technology to support IT operations and infrastructure.

- The Postal Service's highway contract routes (HCR) data retention policies did not require maintenance of detailed data beyond 120 days for historical analyses and for future HCR planning, contract renewal, and contractual or legal challenges by contractors.[7] Additionally, the Postal Service did not develop an overall strategic framework and operational plan for using Global Positioning System technology.

- ███
███
███
███
███
████████████████████████████████████

███
███
████████████████████
███

Unreliable and Inaccurate Data

Data quality and consistency refer to the standards and definitions that guarantee data are reliable, accurate, and effective when stored in a database. This component of the data governance program includes specific policies, organizational structures, and quality assessment methods that allow business users and functional areas to create, download, and store data while minimizing errors and data conflicts. During our review of OIG reports, we noted conditions related to data quality that might have been prevented by a strengthened data governance program. For example:

- Staff did not monitor and correct contract postal unit and Post Office™ meter variances because documented procedures requiring such activities did not exist.[10] We reviewed variances from October 2003 through March 2012 and found 867 meters with usage exceeding reported revenue by about $5.6 million.

- ███
  ███████████ ███
  ███████████████████████ ███████ ██████████████████████
  ███████████████████████████

- Our audit of carrier contributions to revenue generation and customer service showed management might be missing key opportunities to grow revenue due to incomplete data on sales leads.[13]

- Postal Service employees did not always accurately record critical data fields in the Electronic Facilities Management System (eFMS) database.[14] We found owned properties smaller than 10,000 square feet often have inaccurate interior and site square footage measurements. Sixty-eight percent (or 151 of the 222 errors in our sample) occurred primarily because of eFMS system design limitations.[15]

---

[10] *Processing of Meter Activity* (Report Number FT-AR-12-012, dated September 6, 2012).

[11] The Manifest System is accessible from the Point-of-Sale and Advanced Computing Environment workstations.

[12] *U.S. Postal Service Export Controls Monitoring Program* (Report Number FT-MA-12-003, dated September 14, 2012).

[13] *Carrier Contributions to Revenue Generation and Customer Service* (Report Number MS-AR-12-005, dated June 19, 2012).

[14] The eFMS database is the official Postal Service record for real property inventory, used to manage all property-related projects including acquisition, disposal, and repairs.

[15] *Accuracy of the Electronic Facilities Management System* (Report Number DA-AR-12-004, dated September 28, 2012).

Data Inconsistencies within the Enterprise Data Warehouse

EDW is a central, enterprise-wide database that contains information extracted from operational systems. Data governance initiatives look to organize and centralize data warehouses to ensure data are stored correctly. During our review of OIG reports and interviews with employees, we noted conditions related to storing data in and retrieving data from the EDW that may have been prevented by a strengthened data governance program. For example:

- Our review of the chief information officer (CIO) organization's budget and actual expense data for FYs 2010 and 2011, extracted from EDW, revealed misaligned finance numbers and incorrect aggregations of data. The 40 misaligned finance numbers resulted in inaccuracies of $14.9 million of the $1.04 billion year-to-date expenditures.[16]

- Although Finance established an internal team to support Finance organizational activities related to the data warehouse, some other functional areas rely on contractors with no Postal Service operational knowledge. It can be difficult for the contractors to define metrics, templates, and filters for meaningful ad hoc and standard reports.

Insufficient Information Technology Security Measures

The risk and security component area of data governance encompasses risk management policies and monitoring activities implemented within an organization to eliminate unauthorized data access and theft. During our review of OIG reports, we noted conditions that potentially compromise IT security that might have been prevented by a strengthened data governance program. For example:

- Certification and Accreditation (C&A) is a formal security analysis and management approval process used to assess risk before an application is put into production. Management deployed at least 228 applications classified as critical to Postal Service operations into production before completing the required C&A process.[17] This occurred because Corporate Information Security (CIS) did not have the authority necessary to enforce and execute its responsibilities when dealing with individuals outside the CIS reporting structure or whose positions were more senior within the organization.

- ██ ██ ██

---

[16] *Chief Information Officer's Budget Data* (Report Number IT-AR-11-007, dated August 25, 2011).
[17] *State of Security* (Report Number HR-AR-12-005, dated September 12, 2012).
██
██
██

███
███
████████████████████████████████████

- Only 3,878 of the more than 340,000 required users Postal Service-wide (about 1 percent) completed the required initial and annual information security awareness training in FY 2011.[21]

- ██
████████████████████████████████ ██ ████████████
██
███
███
██
███
██

Difficulties with Accessing and Sharing Data

Data utilization describes end-user ability to effectively access, manipulate, share, and create data without assistance of IT personnel. Organizations can provide business user-friendly tools to enable personnel to easily generate, modify, and share analytical reports employing corporate data. During our review of OIG reports, we noted conditions related to data retrieval that may have been prevented by a strengthened data governance program. For example:

- City delivery operations data were voluminous, not 'real time,' and some of the reports were not 'exception-based,' which would facilitate management actions.[23]

- The Postal Service enters into revenue sharing agreements with various partners who are more efficient at providing certain services and products. Management did not maintain a central repository for revenue sharing agreements to ensure timely, efficient, and accurate retrieval of information; and policies and procedures on establishing and monitoring revenue sharing agreements were not clear.[24]

- Enterprise Consumer Care[25] system performance and data issues, including outages and slow performance, have hindered the Postal Service's ability to efficiently address and resolve complaints.[26]

---

[20] *State of Corporate Information Technology Security* (Report Number IT-AR-12-001, dated October 21, 2011).
[21] *Security Training Awareness Program* (Report Number IT-AR-12-008, dated June 25, 2012).
[22] *Virtualization Technology* (Report Number IT-AR-12-007, dated May 18, 2012).
[23] *Delivery Operations Data Usage* (Report Number DR-AR-13-001, dated October 11, 2012).
[24] *Revenue Sharing Agreements* (Report Number FI-AR-12-004, dated September 14, 2012).
[25] Records and tracks customer complaint information for small businesses and residential customers.
[26] *Customer Complaint Resolution Process* (Report Number MS-AR-12-007, dated September 10, 2012).

- Mail processing managers did not always have sufficient information regarding mail processing data. Managers and employees said the availability of data are generally good but could be improved. For example, data from the Intelligent Mail® barcode (IMb) is not readily available for 7 to 10 days. Because this is not a real-time system, most data can only be used for 'after-the-fact' analysis. Additionally, some mailers using IMb have more access to real-time data on mail processing and delivery than is available to Postal Service employees in the plants.[27]

- The Postal Service did not always use Powered Industrial Vehicle Management System (PIVMS)[28] data as intended and, consequently, had not realized all possible efficiency improvements from the system.[29] Specifically, it did not use it to manage equipment operator productivity, schedule preventive maintenance, monitor vehicle battery usage, or identify opportunities to reduce vehicle inventory. Management was not aware of any established national goals or requirements to use the PIVMS to increase operational efficiency, had little confidence in the accuracy of system reports or design features, and had not trained all supervisors who use the PIVMS.

Opportunities to Improve the Postal Service's Data Governance Program

Had the Postal Service implemented a centralized data governance program, we believe many of the issues identified in prior OIG reports might not have occurred. To identify how leading private sector organizations foster and institutionalize data governance programs, we researched best practices and processes with six companies that had advanced data governance frameworks, policies, and practices for an in-depth study. See Appendix B for the rationale for the companies selected.

Our work identified 34 best practices the Postal Service can consider to foster and institutionalize a strong culture and capability for a data governance program. We explain these best practices and provide examples of how the companies apply them in detail in Appendix C. We used these 34 best practices to develop an implementation strategy that is divided into three phases. The phased implementation provides an implementation approach allowing management to establish general, broad policies before taking more specific, technical actions.

Phase I:

1. Assess existing data management practices and policies.

2. Develop organizational structure to support the governance initiative.

3. Appoint data stewards within each business unit.

---

[27] *Timeliness of Mail Processing at Processing and Distribution Centers* (Report Number NO-AR-12-010, dated September 28, 2012).
[28] The PIVMS consists of intelligent wireless devices installed on powered industrial vehicles and client-server software for access control, utilization analysis, real-time location tracking, and many other functions.
[29] *Powered Industrial Vehicle Management System at the Indianapolis Processing and Distribution Center* (Report Number NO-AR-10-004, dated March 29, 2010).

4. Secure buy-in from business units.

Phase II:

5. Develop data performance measures.

6. Take inventory of organizational data.

7. Develop standardized data definitions.

8. Initiate data quality assessments, beginning with top priority data assets.

Phase III:

9. Develop and integrate risk management policies.

10. Develop a data classification system.

11. Develop best-in-class warehousing architecture and management policies.

12. Enhance business user tools and support.

See Appendix C for a more detailed explanation of this implementation approach. The Postal Service can improve the quality and availability of its data by implementing these steps. Adopting and enforcing these practices would:

- Ensure data are reliable, accurate, consistent, and effective.
- Allow consistent definitions for data across the enterprise, minimizing errors.
- Provide a clear protocol and corporate structure.
- Allow stakeholders to access, interact with, create and share data seamlessly.
- Minimize risk of a security breach or data corruption.

While it may not be practical for the Postal Service to implement all 12 steps at once, it should implement them over a defined period. See Appendix D for suggested best practice implementation timeline.

Recommendation

We recommend the chief information officer and executive vice president:

1. Direct the vice president, Information Technology, to implement a formal, enterprise-wide data governance program.

Management's Comments

Management agreed with the finding and, subsequent to their formal response, the recommendation in this report. Management has begun establishing a formal, enterprise-wide, data governance program and has established September 30, 2013, for program implementation.

See Appendix E for management's comments, in their entirety.

Evaluation of Management's Comments

The OIG considers management's comments responsive to the recommendation and corrective actions should resolve the issues identified in the report.

The OIG considers the recommendation significant, and therefore requires OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective action is completed. This recommendation should not be closed in the Postal Service's follow-up tracking system until the OIG provides written confirmation that the recommendation can be closed.

Appendix A: Additional Information

Background

The Postal Service operates one of the largest IT infrastructures in the world and has an inventory of 795 computer applications. Data from many of those applications are collected into data stores and shared widely within the Postal Service. However, employees may not always have access to data they need. In many of the OIG's past audits and risk modeling efforts, the OIG has noticed that postal data are often voluminous but not always organized for ease of use in management decision making.

For FY 2012, the OIG embarked on a series of audits[30] related to how the Postal Service uses data to manage its operations. Most directorates identified one or more audits that specifically addressed the use of data. We coordinated the overall efforts to identify better ways of using data for decision making and workforce planning. In addition, we focused our audit on Postal Service data governance and identified best practices in best-in class companies.

Data governance is the management process ensuring important data assets are formally managed and fully utilized throughout the enterprise. The term data governance describes organizational structures, policies, and practices that govern data management and use. Generally, data governance programs are comprised of core component areas:
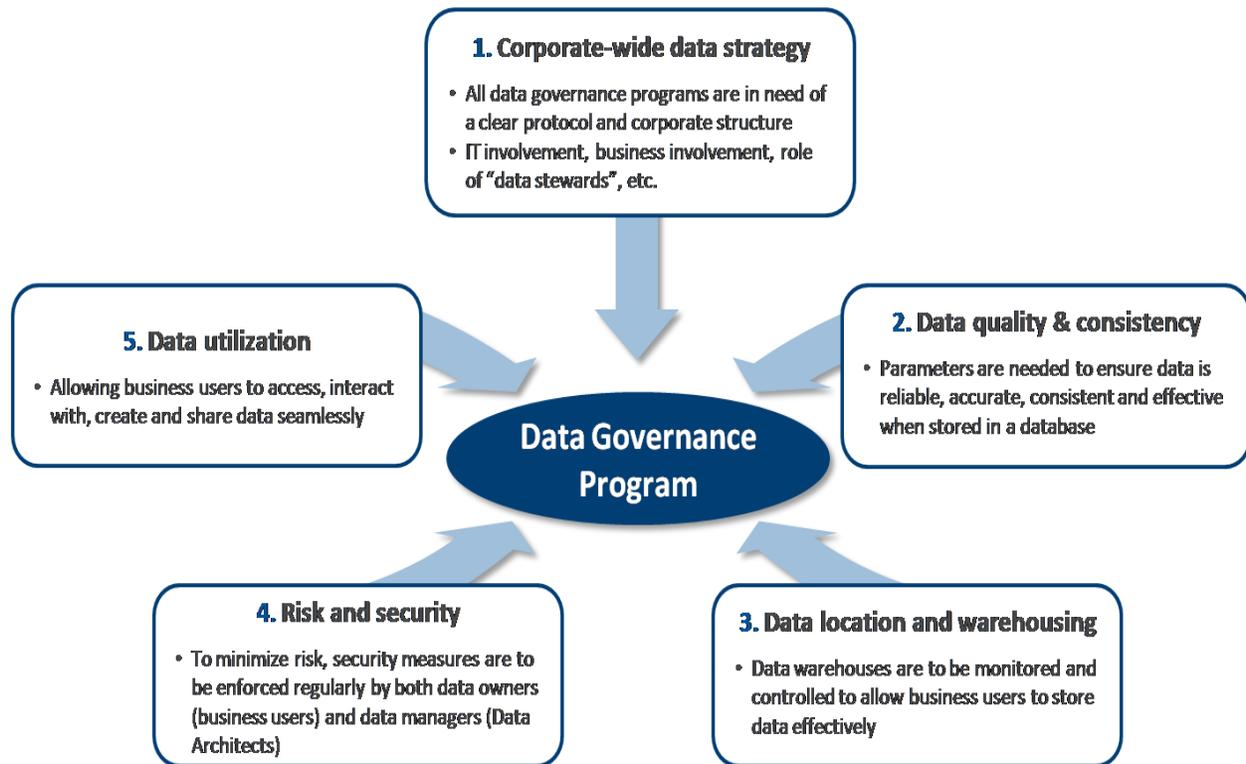
- Corporate-wide data strategy - corporate structure and defined protocol of data governance program.

- Data quality and consistency - parameters and data definitions developed to ensure data are reliable, accurate, consistent, and effective when stored in a database.

- Data location and warehousing - effective storage of data within data warehouses.

- Risk and security - security measures enforced by data owners and data managers to minimize risk.

- Data utilization - capabilities allowing business users[31] to access, manipulate, create, and share data seamlessly.

Figure 1 summarizes the five components of a successful data governance program:

---

[30] There were 14 use-of-data projects announced, of which six reports were issued in FY 2012.
[31] Business users are non-IT personnel that employ and access corporate data.

Figure 1. Five Components of Data Governance

Source: Kaiser Associates.

Enhancements to enterprise-wide data, derived via a formalized data governance program, will lead to more informed decision making for executive management and business users, improved responsiveness to business needs and overall operational savings.

Objective, Scope, and Methodology

Our objective was to determine whether the Postal Service was effectively managing and using data in a manner that assists employees in achieving strategic and operational goals. To accomplish our objective, we:

- Reviewed Postal Service strategies and analyzed the requirements and availability of data to support them.

- Reviewed data governance-related research by reading articles from online resources.

- Provided 'use of data' project teams with audit steps and a questionnaire to collect information from Postal Service officials regarding the organization, quality, and

accessibility of data. We received and reviewed 78 responses from the project teams.

- Reviewed and analyzed OIG reports[32] issued in FYs 2009 through 2012 and identified 148 data-related issues.

- Engaged Kaiser Associates to identify how leading private sector companies foster and institutionalize a data governance program:

  o Conducted secondary research on data governance programs among private organizations to determine the best companies for study. Identified about 20 organizations noted for excellence in data governance.

  o Conducted interviews with data governance practitioners and stakeholders at the 20 identified companies to test the sophistication of each corporate data governance program, in order to narrow the pool of target companies.

  o Identified six companies with advanced data governance programs for an in-depth study.[33]

  o Conducted interviews with internal Postal Service stakeholders to identify current data governance practices and concerns at Postal Service.

  o Analyzed interview findings from all six companies to distill best practices from this research.

- Presented our preliminary list of best practices to Postal Service management and obtained input on the applicability to the agency.

We conducted this performance audit from February 2012 through April 2013 in accordance with generally accepted government auditing standards and included such tests of internal controls as we considered necessary under the circumstances. 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We discussed our observations and conclusions with management on March 12, 2013, and included their comments where appropriate.

We did not test the validity of controls over the Postal Service systems. We relied on the teams that conducted the 'use of data' audits to verify the accuracy of the data with Postal Service managers and other postal data sources. We determined that the data were sufficiently reliable for the purposes of this report.

---

[32] The total number of reports included six data usage reports issued in FY 2012.
[33] In-depth study incorporated multiple primary research interviews with company subject matter experts. Conducted interviews with IT and business personnel in identified companies to outline data governance best practices.

Prior Audit Coverage

In FY 2012, the OIG conducted a series of audits related to how the Postal Service uses data to manage its operations. Although other previously conducted audits identified data-related issues, they were not audits of data governance.

Report Title	Report Number	Final Report Date	Monetary Impact (in millions)
Accuracy of the Electronic Facilities Management System	DA-AR-12-004	9/28/2012	None
Report Results: Postal Service employees did not always accurately record critical data fields. We recommended management modify eFMS to address inconsistency in data entry. Overall, management agreed that eFMS had inconsistent data with incomplete fields in many cases.			
Timeliness of Mail Processing at Processing and Distribution Centers	NO-AR-12-010	9/28/2012	None
Report Results: The Postal Service made progress in improving the timeliness of mail processing by reducing the amount of delayed mail from the previous year and improving service performance for the timely delivery of mail. However, through Quarter 3, FY 2012, about 1.4 billion pieces of mail have been delayed. Management agreed with our recommendations to reduce the amount of delayed mail in the network and ensure that field personnel are properly trained in the color-coding of Standard Mail as well as the counting and reporting of delayed mail in accordance with policies.			

Report Title	Report Number	Final Report Date	Monetary Impact
Use of Data Within Finance and Planning's Field Budget Process	FF-AR-12-005	9/20/2012	None

Report Results:
The Postal Service closed the Southeast Area in February 2011; however, it did not move all the Southeast Area's administrative office's financial data to an active Postal Service area through July 2012. We recommended using financial data to inform senior management and other responsible parties of issues requiring resolution, such as ongoing financial activity and contractual commitments and elevate those issues until resolved. Management agreed with our recommendations.

Report Title	Report Number	Final Report Date	Monetary Impact
Revenue Sharing Agreements	FI-AR-12-004	9/14/2012	$1.4

Report Results:
Management did not implement a process to validate postage and production revenue data or require the alliance partner to provide monthly data on web traffic. Management agreed with our recommendations to implement a process to monitor and communicate goals with revenue sharing agreement partners. However, management disagreed with our recommendation to verify registrations and purchases beyond what is currently in place.

Report Title	Report Number	Final Report Date	Monetary Impact
Customer Complaint Resolution Process	MS-AR-12-007	9/10/2012	$26.4

Report Results:
The Postal Service was not efficiently and effectively resolving customer complaints. Specifically, staff members were closing complaints before customers considered their cases resolved. We recommended the Postal Service develop a mechanism to incorporate customer feedback regarding complaint resolution into the system. Management agreed with the recommendations.

Report Title	Report Number	Final Report Date	Monetary Impact
Contract Management Data – Transportation Contract Support System	CA-AR-12-005	8/9/2012	None

Report Results:
The Transportation Contract Support System contained accurate data for all HCRs we reviewed. Because of the implementation of our prior recommendation regarding contract funding approvals, we did not make any recommendations.

Appendix B: List of Profiled Organizations and Rationale for Selection

Initial research identified six organizations with best-in-class data governance programs for deep-dive best practices research. These organizations can be grouped into three general categories as shown in Table 1:

Category 1: Decentralized Best-in-Class Data Governance Programs: Organizations that maintain a decentralized data governance structure but deploy best-in-class policies around data quality, warehousing, and risk management.

Category 2: Centralized Best-in-Class Data Governance Programs: Organizations that adopted a centralized data governance structure to successfully manage enterprise data.

Category 3: In-Transition Best-in-Class Data Governance Programs: Organizations currently undergoing major changes to internal data governance programs following acquisition of new assets or internal reorganization.

Table 1. List of Profiled Organizations

Company	Category	Rationale for Selection
Company A	Category 1	▪ Advanced data quality and warehousing developed in concert with company growth. ▪ Data quality maintained with expansion to new business sectors. ▪ Best-in-class data risk and security policies.
Company B		▪ Dedicated data governance team, including a steering committee, data stewards, and subject matter experts. ▪ Recently invested in data governance 'toolkit' to improve data consistency, quality, and integration.
Company C		▪ Sophisticated data governance program with codified data management structure. ▪ Data stewards and data architects work with business silos to ensure data quality and consistency.
Company D	Category 2	▪ Best-in-class data governance program with dedicated teams and enterprise-wide data parameters and definitions. ▪ Real-time data update and analytics capabilities.
Company E		▪ Data warehouse steering committee established to oversee data governance program following a merger. ▪ Data warehouse managers ensure data governance structures are maintained by silos.
Company F	Category 3	▪ Formal data governance initiative began in 2011, with investment in data stewards and architects. ▪ Data governance initiative road map preserved following major a acquisition.

Source: OIG analysis.

Appendix C: Data Governance Best Practices

The best practices provided below apply to management of structured and unstructured data.[34] In particular, while systems and processing tools may differ by data type, overall data management policies encompass all data types. The items following summarize five components of a successful data governance program:

 I. Corporate-Wide Data Strategy Best Practices

Initiation of Data Governance

1. Identify and involve key organizational stakeholders in data governance implementation process via a central data governance committee. Best-in-class organizations institute a committee structure to drive the data governance policy creation and implementation process because it allows involvement of a wide range of stakeholders. This structure is favored by executives as it offers opportunities to involve business leaders across the enterprise and help gain traction throughout all business units.

2. Secure executive-level sponsorship to drive adoption of data governance program across the organization — executive-level sponsorship is necessary to drive data governance traction within the organization. As Postal Service's own experience shows, when new policies are introduced without sufficient sponsorship from organizational leadership, they are at best implemented inconsistently, or at worst, disregarded completely. To assure success of a data governance initiative, best-in-class organizations involve an executive-level sponsor to promote and champion the program. This executive serves as an advocate for the program and a last point of escalation if stakeholders do not cooperate with program policies.

3. Demonstrate the business case for a formalized enterprise data governance program to secure buy-in from business area executive sponsors — Data governance stakeholders at best-in-class organizations meet personally with business leaders to demonstrate the advantages (cost savings, productivity benefits) and the business case for data governance and obtain business unit participation. Both group educational sessions and one-on-one meetings with organizational leaders are needed to fully demonstrate the benefits of enterprise-wide data governance and secure organization-wide participation in program implementation.

4. Conduct an analysis of existing data governance policies within individual business units — Rather than building new policies from scratch, best-in-class organizations use existing policies as templates. By conducting surveys, organizations are able to identify existing policies for potential replication on an enterprise-wide level. A data governance initiative can thus minimize the burden of change on business units by

---

[34] Structured data have identifiable structures, most commonly based on methodology of rows and columns. Unstructured data, by comparison, do not have identifiable structures.

simply extending tried and true methods of data management beyond a single silo (or group of silos).

5. Carry out a complete inventory of existing data stored within business unit warehouses — By mapping existing data assets, organizations can best design and implement governance policies. The goal of the inventory process is to determine what data assets the organization currently owns and determine in which locations the assets are stored. With a comprehensive inventory at hand, the data governance committee can accurately assign data management responsibilities, develop a warehousing/storage strategy, and analyze data needs. Without a proper understanding of organizational data holdings, the data governance organization cannot accurately plan data governance program implementation or develop appropriate data accountability policies.

Roles and Responsibilities

6. Assign data steward responsibilities to individuals within business units and the IT organization to develop and oversee data governance policies — Best-in-class organizations assign data steward roles to existing data owners. Data stewards develop policies and drive policy implementation at the business unit level. To minimize the cost and organizational overhaul associated with data governance, organizations typically assign data steward roles to existing personnel. Data stewards must be familiar with IT capabilities as well as the needs of business users to effectively implement data governance policies and monitor policy adherence.

7. Assign program administrator roles with a focus on overseeing data stewardship program — Program administrators supervise data stewards and act as liaisons between data stewards and the data governance committee. This role coordinates the activities of the data stewards and monitors policy implementation activities. Program administrators also assess metrics such as data quality metrics and other key performance indicators (KPI) to evaluate program success.

Data Governance Policy Development

8. Drive data definition and policy creation process via the data governance committee with participation of business unit leaders —The data governance committee serves as the nucleus of policy creation. The council should consult business lines to secure buy-in from the organization's silos. This body is uniquely suited for the task due to the broad-sweeping view of the enterprise operations of its membership, the vested authority within the committee, and its relatively small size. However, stakeholders at best-in-class organizations note that involvement of additional stakeholders, such as executive sponsors or subject matter experts, can significantly augment the policy creation and revision process. Furthermore, the involvement of business units in a review capacity facilitates the creation of enterprise-wide consensus around data governance policies.

9. Assess maturity of data standards in each business unit and set maturity goals according to a defined timeline — Best-in-class organizations assess data standards across business units to create business unit-specific roadmaps for achievement of goals specified by data governance policies. This process begins with a formal, quantitative assessment of data policy and practice maturity within each silo. Data stewards and the data governance committee rate the business unit across a series of data standards, such as Data Quality, Data Integration, Reporting, and so forth, based on predefined policy and data parameter specifications. Then, data stewards and the governance committee determine the governance goals for the business unit over a defined timeline.

10. Tie performance evaluation measures to business unit progress in data governance policy implementation — To hold individuals accountable for data governance implementation, best-in-class organizations incorporate data governance responsibilities into the overall assessment of individual's performance. Best-in-class organizations enact accountability measures for key stakeholders involved in the data governance program, such as data stewards and business unit leaders. Such measures may involve impact on individuals' performance ratings or bonus allocation based on business unit progress in meeting data governance goals. Accountability measures enhance personnel commitment to data governance implementation and link data governance responsibilities to overall personnel performance.

11. Conduct regular educational sessions focused on data governance for all employees that handle data within the organization — Communication of new data governance policies to the business user community is essential for data governance program success. Business users must be trained to properly handle data in accordance with newly created policies. By equipping business users with proper data classification, data storage, and retrieval skills, organizations reduce the workload of IT departments and foster the adoption of data governance policies.

12. Define and utilize metrics to measure data governance initiative performance across the organization — Best-in-class organizations track metrics to measure the effectiveness of data governance policies. This allows stakeholders to quantify and demonstrate the impact of the governance initiative. These metrics, commonly known as KPIs, typically measure data quality, probability of risk, policy compliance, and cost savings. The demonstration of improvement across these areas reinforces the business case for data governance and fosters business unit buy-in and end-user participation.

II. Data Quality and Consistency Best Practices

Priority Data Identification

1. Prioritize a master set of data assets during the onset of data governance initiatives — Organizations define master data, or key business elements, before

introducing data quality initiatives to focus efforts in a strategic manner. Because these data assets represent the organization's priorities, all data cleansing and definition efforts begin with them. Organizations typically task the data governance committee with selection of high priority data assets because the body holds an enterprise-wide view of data priorities.

Data Quality Assessment

2. Identify data quality issues through multilayered data quality scorecard assessments — Best-in-class organizations employ scorecard assessments to test data for errors and provide aggregate-level and detailed views of found quality issues. Designed by IT personnel, scorecards allow business users to analyze the quality level of their data without IT support. If a user's report does not meet established quality standards, the organization bars the user from uploading the report to the warehouse. The user can then use the scorecard to self-diagnose found issues and resubmit for approval. The process thus alerts business users of quality issues and helps maintain the accuracy of data in warehouses.

3. Assign scorecard development responsibility to data stewards — Data stewards are tasked with scorecard development because they have a granular view of business units' data. Data stewards work closely with business users to develop scorecards that are both easy to use and based on parameters customized to the data assets employed by the business unit.

4. Design user-friendly scorecards that allow business users to self-diagnose data quality issues — Scorecards that are user-friendly and accessible allow business users to self-diagnose errors and, consequently, reduce the burden on the IT organizations. If a business user receives a failing score from the quality assessment, the program supplies the rationale and details of why a certain data set or report failed. Business users can then self-service found quality issues and resubmit their data for approval.

5. Customize scorecards based on business units' data assets and needs — Best-in-class organizations create customized scorecards for each business unit to enhance scorecard utility. Because data assets and data usage vary widely from business unit to business unit, a tailored approach to scorecard design is necessary for creation of useful and accurate data quality assessments.

6. Institute a clear schedule for scorecard reporting and assessment by data stewards — All data stewards at profiled companies stress the importance of consistent communication on the issues of data quality. By coordinating closely, data stewards are better able to analyze data quality issues and set quality goals within their business unit. Through meetings with senior data governance stakeholders, data stewards also inform enterprise-wide data quality initiatives with opinions rooted in realities of data quality performance within their business units. Data stewards at interviewed organizations meet weekly to coordinate on data quality initiatives within

a business unit and hold monthly meetings with the data governance committee to discuss enterprise-wide governance initiatives and strategies.

<u>Standardization of Data Definitions</u>

7. Assign data stewards the duty of business glossary development — To ensure data consistency across the enterprise, organizations assign data stewards the role of developing a consistent set of definitions for data assets. The common definitions are then compiled in a business glossary that end-users across business units can reference when creating reports. Data stewards solicit feedback from business users during the process of glossary development. Without sufficient insight or feedback from business users, a business glossary is unlikely to be uniformly adopted across the organization and will thus fail at its primary purpose—the resolution of data consistency issues.

8. Prioritize data glossary development during initial phases of a data governance program — Best-in-class organizations publish a business glossary within 12 months of data governance initiation to stop 'bad habits' of conflicting data use and storage. Organizations administer ongoing end-user surveys and publish a business glossary within this timeframe to immediately align business users on new protocols in creating, storing, and sharing data.

III. Data Location and Warehousing Best Practices

<u>Lifecycle Management</u>

1. Develop clear guidelines for data lifecycle management — Guidelines on data retention and disposal allow organizations to free up storage space by eliminating data that are no longer needed by the user community. These policies also enhance corporate capacity to comply with government and legal policies that require data storage for specified periods. Effective lifecycle management is especially significant for big data[35] because these assets take a large toll on organizational storage capacity.

<u>Data Warehouse Architecture</u>

2. Centralize high priority master data in a single warehouse — Best-in-class organizations with centralized and decentralized warehouse structures house top priority, sensitive data in a single, autonomous warehouse. This allows IT to closely monitor data access around priority data and decreases the threat of a security breach or data corruption. The approach helps maintain a corporation's most important data assets and inspires confidence in business analytics and reporting.

---

[35] Big data describe large data sets that cannot be analyzed via standard relationship databases and analytics tools because of size.

3. Reserve space in the centralized enterprise warehouse for business users to store business-unit specific information — Best-in-class organizations reserve business unit-specific storage space to allow business users to store and rapidly retrieve information used by their silo. Business units can thus store specialized data, such as department specific summary tables or aggregations, in enterprise warehouses where it can be properly monitored and managed by the IT organization. Organizations that have or are moving towards a centralized warehousing structure, like Postal Service, thus inhibit business units for establishing siloed data marts without proper IT supervision.

4. Architect warehouses to automatically update with incoming data to guarantee data are relevant and up-to-date — Best-in-class data warehouses are engineered to automatically pull updated data from business users and servers, guaranteeing that data are current. Automated data upload stream data through a consistent channel, optimizing warehouse performance and enabling data users to upload data instantly. As a result, warehouses can support real-time business analytics functionality.

Data Warehouse Management Roles

5. Dedicate a team of IT professionals to manage data warehouses and act as a liaison between IT and business directors — Best-in-class corporations employ data warehouse groups to manage the ongoing maintenance and continuous improvement of enterprise warehouses (including central and distributed warehouses). Such groups are comprised of data engineers and architects who are well-versed in warehouse architecture design and understand the business needs of the organization. Team members maintain close contact with the data governance committee and work to develop new technical policies and procedures to enhance end-user experiences. A data warehouse group thus enables data governance directors to better understand the technical ramifications of governance policies and ensure business user needs are met.

6. Appoint IT employees to monitor data queries and enforce the established search protocols — Best-in-class organizations develop clear protocols for search queries to bar business users from unnecessarily requesting large amounts of data and placing a burden on the overall data retrieval system. Organizations then appoint IT staff to monitor data queries and hold business users who do not follow protocols accountable. This enforcement model drastically lowers the likelihood of business user circumvention of data query policies.

Data Classification

7. Develop a data classification system to sort data into distinct tiers based on priority — Best-in-class organizations create automated data classifications systems to sort data into distinct tiers based on sensitivity and relevance. The tier definitions are developed by the data governance committee with participation from the business user community. Following definition development, the IT organization

automates the classification process, tagging all incoming data with appropriate tier classification. This allows IT to apply storage, lifecycle management, and quality control policies specific to the data type within the tier.

IV. Risk and Security Best Practices

1. Merge established risk management policies with data management guidelines developed under the auspices of a data governance program — Data governance committees at interviewed organizations work closely with risk management offices to standardize security policies across the enterprise and incorporate them into overall data management guidelines. In fact, organizations often prioritize data risk management as one of the key tenets of the data governance program. Data governance policies and organizational structures reinforce existing security measures and centralize them across silos. Accordingly, program stakeholders assume responsibilities for security assessment and monitoring.

2. Set clear guidelines for data access provisioning and conduct regular reviews of data access rights — To minimize risk of unauthorized data access and security breach, best-in-class data governance programs establish a clearly defined process for users to gain data access rights. The process guidelines are distributed to all silos and implemented consistently throughout the organization. IT organizations then routinely review data access rights on a predetermined schedule to further minimize risk.

V. Data Utilization Best Practices

1. Conduct regular surveys of end-user needs to enhance data utilization — Best-in-class data governance organizations conduct routine assessments of business user opinions to understand where current tools and policies fall short. This process allows organizations to better meet business analytics needs of business users and enhance personnel and business process efficiency. Profiled programs keep a close pulse on end-user opinion, testing whether deployed tools or implemented policies are beneficial to the enterprise's data consumers. This allows committees to quickly identify areas for improvement. Well-informed strategies then lead to optimized data utilization and end-user efficiency.

2. Develop technology resources that direct business users to appropriate parties for data retrieval and IT issues — Data governance committees at interviewed organizations work alongside IT departments to develop an IT catalogue that business users can use when they require assistance with data governance procedures, data quality policies, and storage/retrieval issues. This allows business users to save time when experiencing issues and quickly contact the relevant party for their needs. In turn, the IT department is not inundated with multiple requests from business users.

3. Develop user-friendly metadata[36] views to enhance warehouse data queries — Metadata management technology allows companies to better understand, collect, catalog, and manipulate enterprise data. It also provides a clear view of the information contained in data warehouses, accurately grouping related data and excluding irrelevant data. As a result, metadata expedite and simplify data searches, directly benefiting the business user community. Metadata management is especially significant in improving user ability to search big data because of the sheer size of these assets. Metadata also enables IT departments to automate big data monitoring, enhancing risk and quality management of this data type.

4. Design business intelligence dashboard tools to help business users view and analyze needed data — Best-in-class organizations design dashboards to allow for superior data analytics and increase data utilization by the business user community. Dashboards present data in a user-friendly format, employing charts and tables that can be easily manipulated by the user without the risk of data corruption. Dashboards are developed by IT with input from business users who specify what data views are most actionable for their business needs.

5. Designate an IT representative to every business user project team to assist with IT issues and concerns — Project-driven organizations with strong governance programs often assign an IT representative with a strong commitment to the organization's data governance protocols to specific business projects to serve as a liaison between the project team and IT staff. These IT representatives assist business users with access rights and data retrieval for the duration of their project. Business users thus benefit from direct and rapid assistance of the dedicated IT representative. The IT representative meanwhile monitors and enforces data retrieval and storage protocols, propagating the goals of the data governance program.

---

[36] Metadata are structured information that describe, explain, locate, or otherwise make it easier to retrieve, use, or manage an information resource.

Appendix D: Suggested Best Practice Implementation Timeline

Best-in-class organizations create a detailed roadmap for best practice implementation as part of the data governance initiative. Based on the experiences and recommendations of interviewed organizations, we developed a suggested implementation roadmap, divided into three phases of varying durations. Each phase contains four key processes that should be executed in sequential order. All best practices contained in this document have been organized under these process elements, as illustrated in Figure 2:

Figure 2. Best Practices by Process Element Category
Phase I: First 6 Months

Process Step	Best Practice	Component Area
Step 1	Conduct an analysis of existing data governance policies within individual business units.	Corporate-wide data strategy
Step 2	Identify and involve key organizational stakeholders in data governance implementation process via a central data governance committee.	Corporate-wide data strategy
Step 2	Secure executive-level sponsorship to drive adoption of data governance program across the organization.	Corporate-wide data strategy
Step 2	Assign program administrator roles with a focus on overseeing data stewardship program.	Corporate-wide data strategy
Step 3	Assign data steward responsibilities to individuals within business units and the IT organization to develop and oversee data governance policies.	Corporate-wide data strategy
Step 4	Demonstrate the business case for a formalized enterprise data governance program to secure buy-in from business leaders.	Corporate-wide data strategy
Step 4	Drive data definition and policy creation process via the data governance committee with participation of business unit leaders.	Corporate-wide data strategy
Step 4	Conduct regular educational sessions focused on data governance for all employees that handle data within the organization.	Corporate-wide data strategy

Source: OIG analysis.

Phase II: 6-12 Months

Process Step	Best Practice	Component Area
Step 1	Define and utilize metrics to measure data governance initiative performance across the organization.	Corporate-wide data strategy
Step 1	Tie performance evaluation measures to business unit progress in data governance policy implementation.	Corporate-wide data strategy
Step 1	Assess maturity of data standards in each business unit and set maturity goals according to a defined timeline.	Corporate-wide data strategy
Step 2	Carry out a complete inventory of existing data stored within business unit warehouses.	Corporate-wide data strategy
Step 3	Assign data stewards the duty of business glossary development.	Data quality and consistency
Step 3	Prioritize data glossary development during initial phases of a data governance program.	data quality and consistency
Step 4	Prioritize a master set of data assets during the onset of data governance initiatives.	Data quality and consistency
Step 4	Identify data quality issues through multilayered data quality scorecard assessments.	Data quality and consistency
Step 4	Assign scorecard development responsibility to data stewards.	Data quality and consistency
Step 4	Design user-friendly scorecards that allow business users to self-diagnose data quality issues.	Data quality and consistency
Step 4	Customize scorecards based on business units' data assets and needs.	Data quality and consistency
Step 4	Institute a clear schedule for scorecard reporting and assessment by data stewards.	Data quality and consistency

Source: OIG analysis.

Phase III: 12-24 Months

1 Develop and integrate risk management policies	2 Develop a data classification system	3 Develop best-in-class warehousing architecture and management policies	4 Enhance business user tools and support

Process Step	Best Practice	Component Area
Step 1	Merge established risk management policies with data management guidelines developed under the auspices of a data governance program.	Risk and security
Step 1	Set clear guidelines for data access provisioning and conduct regular reviews of data access rights.	Risk and security
Step 2	Develop a data classification system to sort data into distinct tiers based on priority.	Data location and warehousing
Step 3	Develop clear guidelines for data lifecycle management.	Data location and warehousing
Step 3	Centralize high priority master data in a single warehouse.	Data location and warehousing
Step 3	Reserve space in the centralized enterprise warehouse for business users to store business-unit specific information.	Data location and warehousing
Step 3	Architect warehouses to automatically update with incoming data to ensure relevant and up-to-date data.	Data location and warehousing
Step 3	Dedicate a team of IT professionals to manage data warehouses and act as a liaison between IT and business directors.	Data location and warehousing
Step 3	Appoint IT employees to monitor data queries and enforce the established search protocols.	Data location and warehousing
Step 4	Conduct regular surveys of end-user needs to enhance data utilization.	Data utilization
Step 4	Develop technology resources for business users that helps navigate them towards appropriate parties for data retrieval and IT issues.	Data utilization
Step 4	Develop user-friendly metadata views to enhance warehouse data queries.	Data utilization
Step 4	Design dashboard tools to help business users view and analyze needed data.	Data utilization
Step 4	Designate an IT representative to every business user project team to assist with IT issues and concerns.	Data utilization

Source: OIG analysis.

Appendix E: Management's Comments

ELLIS A. BURGOYNE
CHIEF INFORMATION OFFICER
EXECUTIVE VICE PRESIDENT

**UNITED STATES
POSTAL SERVICE**

April 15, 2013

JUDITH LEONHARDT
DIRECTOR, AUDIT OPERATIONS

SUBJECT: U.S. Postal Service Data Governance (Report Number:DP-AR-13-DRAFT)

Thank you for the opportunity to review and comment on the U.S. Postal Service Data Governance draft audit report.

Management Response: Management agrees with the finding in this report. The subject report and this response contain information related to potential vulnerabilities that, if released, could be exploited and cause substantial harm to the U.S. Postal Service. The Chief Information Officer and Executive Vice President requests that sections *Inconsistent Corporate-wide Data Strategy* (page 3), *Unreliable and Inaccurate Data* (page 4) and *Data Inconsistencies in the Enterprise Data Warehouse* (page 5) of the report should be considered as classified, restricted, and exempt from disclosure under the Freedom of Information Act.

Management agrees with the calculations referenced below. In addition, management believes that the referenced calculations, if released, could be exploited and cause substantial harm to the U.S. Postal Service. The Chief Information Officer and Executive Vice President requests that the below referenced sections be considered as classified, restricted, and exempt from disclosure under the Freedom of Information Act:

> "Staff did not monitor and correct contract postal unit and Post Office™ meter variances because documented procedures requiring such activities did not exist. We reviewed variances from October 2003 through March 2012 and found 867 meters with usage exceeding reported revenue by about $5.6 million.
>
> The Postal Service did not have a consistent strategy or approach for determining the risks and benefits of implementing cloud computing technology. Having a consistent strategy and approach to cloud computing technology would allow management to develop an optimal cloud computing model to increase business and operating efficiency and lower infrastructure cost. We estimated an annual potential cost savings of $2.6 million using cloud computing technology to support IT operations and infrastructure.

2

Our review of the Chief Information Officer and Executive Vice President (CIO) organization's budget and actual expense data for FYs 2010 and 2011, extracted from EDW, revealed misaligned finance numbers and incorrect aggregations of data. The 40 misaligned finance numbers resulted in inaccuracies of $14.9 million of the $1.04 billion year-to-date expenditures."

Recommendation 1:
We recommend the Chief Information Officer and Executive Vice President:
Direct the vice president, Information Technology, to implement a formal, enterprise-wide data governance program.

Management Response/Action Plan:

Management agrees with the findings in the report and has begun the process to establish a formal, enterprise-wide data governance program. Management has created a framework to establish the program which identifies a high-level governance model, the executive sponsors, and is in the process of identifying the data stewards for both IT and the business as well as key activities that will take place to implement the program. Establishment of a formal data management program throughout the enterprise will include selection of work-flow processes, creation of an organizational structure, identification of key team members as well as definition of roles, responsibilities and funding needs. The approach to establishment of this program will be presented to U.S. Postal Service Executive Leadership Team (ELT) through the DRIVE program. The expected target date for initial implementation of the enterprise data management governance program is the end of the 2013 fiscal year. Further detailed implementation milestones will be determined based upon the final scope and governance processes approved by the ELT.

Target Implementation Date:

September 30, 2013

Responsible Official:

Joe Gabris, Acting Manager, IT Strategy and Compliance

Ellis Burgoyne

Ellis A. Burgoyne

cc: James P. Cochrane
     John T. Edgar
     Corporate Audit and Response Management