



Office of Inspector General | United States Postal Service

Audit Report

Cybersecurity Decision Analysis Reports Review

Report Number IT-AR-19-002 | November 19, 2018



Table of Contents

Cover	
Highlights.....	1
Objective	1
What the OIG Found.....	1
What the OIG Recommended.....	1
Transmittal Letter	2
Results.....	3
Introduction/Objective	3
Background.....	3
Finding #1: Operating Expense Budget.....	4
Recommendation #1.....	5
Finding #2: DAR II Expense Tracking	6
Recommendation #2	6
Management's Comments.....	6
Evaluation of Management's Comments	7
Appendices	8
Appendix A: Additional Information.....	9
Scope and Methodology.....	9
Prior Audit Coverage.....	9
Appendix B: Management's Comments.....	10
Contact Information	12

Highlights

Objective

Our objective was to assess whether Decision Analysis Reports (DAR) I and II cybersecurity investments' stated performance metrics aligned with the Corporate Information Security Office (CISO) strategic and cost objectives.

To establish a sound cybersecurity foundation, the U.S. Postal Service has made significant investments in information security. In 2015, the Postal Service approved [REDACTED] million in investments; [REDACTED] million for Cybersecurity DAR I and [REDACTED] million for Cybersecurity Improvements DAR II.

In addition to these investments, these DARs included projected operating expenses of [REDACTED] million from fiscal years (FY) 2016 through 2022. Capital and deployment investments for DARs I and II were completed in November 2015 and September 2017, respectively. Ongoing operating expenses for each DAR continue to be incurred.

Each DAR's total approved investment amount is comprised of a capital investment, deployment investment expenses, and first-year operating expenses. Thereafter, an annual budget must be submitted for each year's operating expenses for each DAR.

What the OIG Found

Overall, the Postal Service's investment strategies have been effective in strengthening its enterprise cybersecurity program and achieving strategic objectives. However, the Postal Service could enhance its financial commitments to the long-term capabilities of administering the cybersecurity program by establishing continued budgets to fund annual operating expenses.

We found the Postal Service uses the DAR process to approve, monitor, and fund operating expenses for cybersecurity investments. However, expenses associated with day-to-day operations to sustain ongoing cybersecurity operations are not considered to be investments per Postal Service investment policy. These operating expenses are necessary and administrative in nature to sustain ongoing cybersecurity operations and are not expected to end. Examples of such operating expenses are rent, software licenses and services, and employee and contractor support.

This occurred because the Postal Service has not performed long-range planning and administering the cybersecurity program. Without an ongoing cybersecurity operating budget, the Postal Service may not be able to appropriately secure the enterprise to ensure uninterrupted service delivery, preserve customer and employee trust, and maintain competitive products in the digital marketplace. Additionally, the use of multiple finance numbers to manage the investments has made it difficult for management to exercise oversight of the DARs.

We also found the CISO did not track line item expenditures with sufficient detail throughout the DAR II investment. This occurred because CISO considered all approved operating expenses as a single budget and not subject to annual budgetary limits. As a result, CISO could not readily determine whether the [REDACTED] million overspending in DAR II was operational or deployment expenses. Additionally, by not tracking detailed project expenditures, the sponsor would not be able to evaluate achieved benefits, identify and implement corrective action, and document any required operational or capital investment modifications.

What the OIG Recommended

We recommended management create and execute a program/administrative budget to adequately plan and administer an ongoing cybersecurity program and manage and track DAR II spending against cash flow line items throughout the investment.

Transmittal Letter

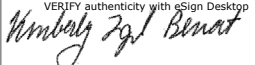


OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

November 19, 2018

MEMORANDUM FOR: GREGORY S. CRABB
VICE PRESIDENT, CHIEF INFORMATION SECURITY
OFFICER

LUKE T. GROSSMANN
VICE PRESIDENT, FINANCE AND PLANNING

E-Signed by Kimberly Benoit
VERIFY authenticity with eSign Desktop


FROM: Kimberly F. Benoit
Deputy Assistant Inspector General for Technology
and Data Analysis

SUBJECT: Audit Report – Cybersecurity Decision Analysis Reports
Review (Report Number IT-AR-19-002)

This report presents the results of our audit of the U.S. Postal Service Cybersecurity Decision Analysis Reports Review (Project Number 18TG009MI000).

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Jason Yovich, Director, Information Technology, or me at 703-248-2100.

Attachment

cc: Postmaster General
Corporate Audit Response Management

Results

Introduction/Objective

This report presents the results of our self-initiated audit of the Cybersecurity Decision Analysis Reports (DAR) Review (Project Number 18TG009MI000). Our objective was to assess whether DAR I and DAR II cybersecurity investments' stated performance metrics aligned with the Corporate Information Security Office's (CISO) strategic and cost objectives.

Background

The CISO is responsible for detecting, preventing, and protecting the Postal Service's infrastructure against cyberthreats that could disrupt operations to 45,000 retail terminals, 2,837 retail kiosks, 8,500 pieces of mail processing equipment, USPS.com, and more. The CISO responds to an average of [REDACTED] cyberthreats and incidents every month.

To establish a sound cybersecurity foundation, the Postal Service has made significant investments in information security. In 2015, the Postal Service approved \$[REDACTED] million in investments: DAR I for [REDACTED] million and DAR II for \$[REDACTED] million. See Table 1 for an investments summary. In addition to these investments, the two DARs included projected operating expenses of [REDACTED] million from fiscal years (FY) 2016 through 2022 as shown in Table 2. In January 2018, the Postal Service approved an additional [REDACTED] million for DAR III to enhance the improvements made in cybersecurity resulting from DARs I and II. The estimated project completion date is February 2020. Because the deployment is ongoing, we did not evaluate DAR III as part of this audit.

Table 1. Investments Summary (in millions)

DAR Title	Capital Investment	Deployment Expense	First-Year Operating Expense	Total
Cyber Security DAR I	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Cybersecurity Improvements DAR II	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Total	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Source: DAR I dated February 20, 2015; DAR II dated July 27, 2015.

Corporate Information Security Office...

is responsible for:



Detecting



Preventing



Protecting

the Postal Service's infrastructure against cyberthreats that could disrupt operations to:

**Retail
Terminals**

**Retail
Kiosks**

**Mail
Processing
Equipment**

USPS.com

and more.

Table 2. Fiscal Years Projected Operating Expenses Summary (in millions)

DAR Title	2016	2017	2018	2019	2020	2021	2022	Total
Cyber Security DAR I	████	████	████	████	████	██	██	████
Cybersecurity Improvements DAR II	█	████	████	████	████	████	████	████
Total	████	████	████	████	████	████	████	████

Source: DAR I dated February 20, 2015; DAR II dated July 27, 2015.

The Postal Service completed capital and deployment investments for DARs I and II in November 2015 and September 2017, respectively. Ongoing operating expenses for each DAR continues.

For a project with total costs over \$5 million, the project sponsor must prepare and submit a DAR to the Investment Review Committee (IRC) to obtain project funding, which is subjected to the Postmaster General's approval. The purpose of a DAR is to ensure investments are properly documented, reviewed, and approved. The DAR defines the problem or opportunity to be solved and quantifies the need for the expenditures. It must provide sufficient detail, including backup documentation, to enable the approving authorities to make an informed decision. Each DAR's total investment approval amount is comprised of a capital investment, deployment investment expenses, and first-year operating expenses. Thereafter, an annual budget must be submitted for each year's operating expenses for each DAR.

Finding #1: Operating Expense Budget

Overall, the Postal Service's investment strategies have been effective in strengthening its enterprise cybersecurity program. However, the Postal Service could enhance its financial commitment to administer the cybersecurity program by using the program/administrative budget¹ process to continue funding annual operating expenses.

We found that while the Postal Service has used the DAR process to fund annual operating expenses for DARs I and II, expenses associated with day-to-day operations are not considered to be investments per Postal Service policy.²

These operating expenses are administrative in nature, recurring, and necessary to sustain an ongoing cybersecurity operation (e.g., rent, software licenses and services, and employee and contractor support). To that point, Table 3 shows the CISO has a non-cybersecurity DAR budget of █████ million, which is 21 percent of the total █████ million³ total budget for FYs 2015 – 2018.

“ The Postal Service could enhance its financial commitment to administer the cybersecurity program.”

¹ Program budget is for recurring projects that need ongoing funding. Administrative budget is annual funding for salaries and benefits and non-personnel expenses.

² Handbook F-66E, *Investment Policies and Procedures — Postal Support and Information Systems*, dated December 2005.

³ This total includes DAR III budget to show the total DAR budget as compared to total CISO budget.

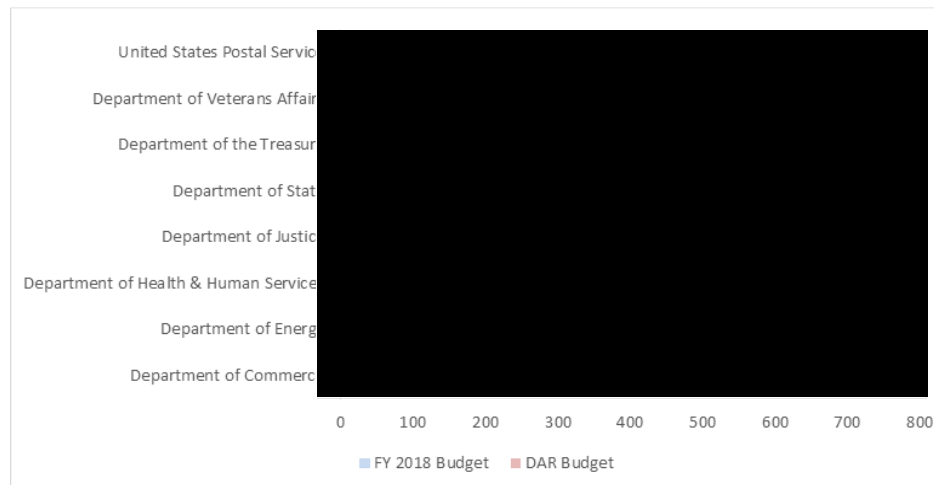
Table 3. CISO Budget⁴ (in millions)

Fiscal Year	Cybersecurity DAR Budget	Percentage	Other Budget	Percentage	Total Budget
2015	████	████	████	████	████
2016	████	████	████	████	████
2017	████	████	████	████	████
2018	████	████	████	████	████
Total	████	████	████	████	████

Source: Postal Service Electronic Data Warehouse (EDW), as of September 18, 2018.

As shown in Figure 1, we found the FY 2018 cybersecurity budgets for eight federal agencies range from █████ million to █████ million. For the same period, the Postal Service's CISO budget, without cybersecurity DARs funding, is \$████ million.

Figure 1. FY 2018 Federal Agencies' Cybersecurity Budgets (in millions)



Source: FY 2019 budget of the U.S. government.⁵

In addition, the CISO experienced cybersecurity operating expense funding issue in FY 2017. Specifically, DAR I operating expenses of █████ million was not funded. As a result, the CISO covered those expenses with the DAR II funding to ensure operations continued.

This occurred because the Postal Service has not performed financial long-range planning and administering the cybersecurity program. Without an ongoing cybersecurity operating budget, the Postal Service may not be able to appropriately secure the enterprise to ensure uninterrupted service delivery, preserve customer and employee trust, and maintain competitive products in the digital marketplace. Additionally, the use of multiple finance numbers to manage the investments has made it difficult for management to exercise oversight of the DARs.

Recommendation #1

The Vice President, Finance and Planning, in coordination with the Vice President, Chief Information Security Officer, create and execute a program/administrative budget to adequately plan and administer an ongoing cybersecurity program.

⁴ This is the entire CISO budget, which includes cybersecurity DAR investments, non-cybersecurity DAR investments, and other program/administrative budgets related to CISO organization activities.

⁵ <https://www.gpo.gov/fdsys/pkg/BUDGET-2019-PER/pdf/BUDGET-2019-PER.pdf>

Finding #2: DAR II Expense Tracking

We found the CISO did not track line item expenditures throughout the DAR II investment with a sufficient level of detail. According to Postal Service policy,⁶ the sponsor must track both initial and ongoing cash outflows of a project exactly as they are listed in the DAR.

This occurred because the CISO considered all DARs' approved operating expenses, including future years' projections, as a single budget and these expenses were not subject to annual budgetary limits if spending was less than the DARs' total approved amount. As a result, the CISO could not readily determine whether the [REDACTED] million overspending in DAR II, as shown in Figure 2, was operational or deployment expenses. Additionally, by not tracking detailed project expenditures, the sponsor would not be able to evaluate achieved benefits, identify and implement corrective action, and document any required operational or capital investment modifications.

Figure 2. DAR II Expenses - Planned vs. Actual (in millions)



Source: DAR III, dated January 2, 2018.

During the audit, Postal Service reconciled DAR II spending to cash flow line items for FYs 2016 and 2017 and was able to determine operational versus

deployment expenses. In addition, CISO management stated they have developed a process to track detailed spending at the project level for DAR III and may use the process to continue DAR II tracking. CISO management also stated that spending needs for contracting resources to maintain ongoing cybersecurity work necessitated them using the DAR II budget to fund DAR III expenses until May 2018, when DAR III funding was made available. The CISO is currently working with Finance and Planning to transfer these expenditures from DAR II to DAR III.

Recommendation #2

The Vice President, Chief Information Security Officer, manage and track Decision Analysis Report II spending against cash flow line items throughout the investment.

Management's Comments

Management agreed with all recommendations in the report.

Regarding recommendation 1, management agreed to deploy and fund a new program/administrative budget for its cybersecurity program. Management will move already planned ongoing operating costs for DARs I and II to this new program/administrative budget. The target implementation date is January 31, 2019.

Regarding recommendation 2, management agreed to document a process to track and monitor detailed project level spending for DAR II. The target implementation date is January 31, 2019.

Management disagreed with the OIG's assessment that the Postal Service did not perform long-range planning in administering the cybersecurity program. Management stated the DAR process requires long-range spending estimates, including both capital and expense investments and ongoing operating costs for the five-year analysis period of the DAR.

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

⁶ Handbook F-66, General Investment Policies and Procedures, November 2005, updated with Postal Bulletin revisions through October 11, 2007.

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.

Regarding management's comments about the DAR process requiring long-range spending estimates, the DAR process does include estimating ongoing operating expenses. However, these operating expenses should be related to the investment and are requested each year. During our audit, we identified expenses associated with day-to-day operations that were not an appropriate use of the investment process. It is the OIG's position that a program/administrative budget rather than a capital investment be used to appropriately secure the enterprise to ensure uninterrupted service delivery, preserve customer and employee trust, and maintain competitive products in the digital marketplace.

All recommendations require OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. 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 below to navigate to the section content.

Appendix A: Additional Information.....	9
Scope and Methodology	9
Prior Audit Coverage	9
Appendix B: Management’s Comments.....	10

Appendix A: Additional Information

Scope and Methodology

The scope of this audit was DAR I dated February 20, 2015, and DAR II dated July 27, 2015. DAR III, dated December 11, 2017, was not part of this audit because deployment is ongoing.

To accomplish our objective, we:

- Reviewed a judgmental sample of cybersecurity related contracts to determine:
 - Whether mandatory and information technology-specific clauses were listed in the contracts;
 - The validity of the competitive and non-competitive contracts justification documents;
 - Reasonableness of contracted labor rates as compared to GSA labor rates; and
 - Key personnel listed on the contracts performed contract works.
- Compared DARs actual spending to budgets and interviewed key personnel to determine if overspending occurred and if proper procedures were followed.
- Reviewed Postal Service's quarterly *DAR Compliance Reports*⁷ to determine if performance metrics were tracked according to Handbook F-66.

- Reviewed a random sample of closed recommendations⁸ to determine if corrective action was appropriate and sufficient.
- Determined whether employees followed Handbooks F-66 and F-66E when developing and executing the DARs.

We conducted this performance audit from March through November 2018, 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 October 15, 2018, and included their comments where appropriate.

We assessed the reliability of DARs I and II projected and actual expenditure data by evaluating the expenditures in the EDW⁹ and reviewed the data for completeness, reasonableness, accuracy, and validity. Additionally, we discussed the data with knowledgeable Postal Service officials. We determined that the data were sufficiently reliable for the purposes of this report.

Prior Audit Coverage

The OIG did not identify any prior audits or reviews directly related to the objective of this audit within the last five years.

⁷ The report is prepared quarterly from project approval until 18 months after final deployment/completion. The purpose of the report is to track the progress of a project and its compliance with the approved plan. We reviewed Quarter (Q) 3, 2016, and Q2, 2018.

⁸ There were over 600 recommendations from business partner assessments and other internal and external entities that provided the CISO a security roadmap for remediation efforts and mapped to information security strategic objectives.

⁹ A repository for all data and the central source for information on retail, financial, and operational performance.

Appendix B: Management's Comments



November 6, 2018

MONIQUE COLTER
DIRECTOR, AUDIT OPERATIONS

SUBJECT: Cybersecurity Decision Analysis Reports Review,
Report Number IT-AR-19-DRAFT

Thank you for the opportunity to review and comment on the Office of Inspector General (OIG) *Cybersecurity Decision Analysis Reports Review* audit. This audit recognizes that the U.S. Postal Service's investment strategies have been effective in strengthening its enterprise cybersecurity program and achieving its strategic objectives.

While we agree with the recommendations of the report, we disagree with the characterization found within the report that "the Postal Service has not performed long-range planning and administering the cybersecurity program." The Decision Analysis Report (DAR) business case process requires long-range spending estimates. These estimates include both capital and expense investments as well as ongoing operating costs through the five year analysis period of the business case. To date, the Postal Service and the Corporate Information Security Office (CISO) have made significant progress in managing the cybersecurity investment process and are committed to further strengthening this process to align the organization's cybersecurity performance metrics with its strategic and cost objectives.

In fiscal year (FY) 2017, CISO accelerated spending on DAR II to bring in critical and urgent cybersecurity capabilities for the Postal Service. CISO plans to remain within the [REDACTED] million approved budget for the seven year DAR II period.

Moving forward, management will continue enhancing its financial commitment for a sustainable cybersecurity program. Additionally, CISO will document a process to track and monitor detailed DAR project expenditures to more effectively evaluate achieved benefits, identify and implement any necessary corrective action, and document any operational or capital investment modifications.

Recommendation [1]:

The Vice President, Finance and Planning, in coordination with the Vice President, Chief Information Security Officer, create and execute a program/administrative budget to adequately plan and administer an ongoing cybersecurity program.

Management Response/Action Plan

Management agrees with the recommendation for the cybersecurity program. The Postal Service has invested over \$[REDACTED] million in Cybersecurity DAR programs since FY2015. In FY2018, the Postal Service expanded its long range plans for Cybersecurity through Cybersecurity DAR III which increased cyber-related spending by an additional [REDACTED] million over the DAR's cash flow. Based on current long-term forecasts, the Postal Service will spend over [REDACTED] million on cybersecurity over the next 6 years.

As suggested by the recommendation, Cybersecurity DARs I & II will have their already planned ongoing operating costs moved into new program/administrative budgets which are logically aligned with related business functions and operations as warranted in this case. Finance and Planning and the Chief Information Security Officer functions will work together to create a plan to deploy and fund the new program/administrative finance numbers to facilitate the future tracking of cybersecurity spending.

Target Implementation Date: January 31, 2019

Responsible Officials: Manager, Capital Investments and Business Analysis
Manager, CIO Finance

Recommendation [2]:

The Vice President, Chief Information Security Officer, manage and track Decision Analysis Report II spending against cash flow line items throughout the investment.

Management Response/Action Plan

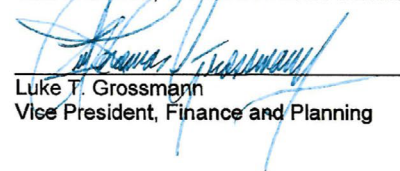
Management agrees with the intent of this recommendation. Management considers the financial tracking, called for in the report, beyond the customary accounting practices of the Postal Service. CISO will document a process to track detailed spending at the project level under DAR II.

Target Implementation Date: January 31, 2019

Responsible Official: Deputy Chief Information Security Officer



Gregory S. Crabb
Vice President, Chief Information Security Office



Luke T. Grossmann
Vice President, Finance and Planning



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

Contact us via our [Hotline](#) and [FOIA](#) forms.

Follow us on social networks.

Stay informed.

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