Office of Inspector General | United States Postal Service

Audit Report

U.S. Postal Service's Implementation of Enterprise Risk Management

Report Number 21-235-R22 | May 19, 2022

Table of Contents

Highlights

Background

The primary mission of the U.S. Postal Service's enterprise risk management (ERM) program is to provide reasonable assurance that significant risks to and opportunity losses for the organization are systematically and effectively identified, evaluated, and mitigated where appropriate. The organization's ERM Operating Charter (Charter) establishes the Executive Leadership Team in general and the Chief Financial Officer (CFO) in particular as having the responsibility for aligning the organization's goals, defining roles, and driving progress with oversight by the Board of Governors' Audit and Finance Committee. The ERM program is led by Finance, as directed by the CFO and the Vice President, Controller.

What We Did

Our objective was to assess the effectiveness of the Postal Service's implementation of the Charter and identify opportunities to improve the ERM program.

What We Found

While the Postal Service effectively implemented several aspects of the Charter, we identified elements related to annual reviews, program targets, and defined responsibilities that were not fully implemented. Specifically, we noted that management had not reviewed the Charter at least annually or established a formal schedule for periodic reviews, established targets for risk mitigation and resource allocation, or defined risk management responsibilities across the organization.

Further, the Postal Service ERM program incorporates several good practices identified by federal and industry guidance; however, we identified opportunities for improving the program. These opportunities include identifying and inventorying existing risk management practices, enhancing risk reporting, and assessing the program to develop the next phase of Postal Service ERM.

Recommendations

We recommend management review and update the ERM Operating Charter to reflect the current needs of the organization and implement the revised Charter and consider the opportunities for improvement discussed in this report and identify actions to further develop the ERM program.

Transmittal Letter

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

May 19, 2022

MEMORANDUM FOR: JOSEPH CORBETT
CHIEF FINANCIAL OFFICER AND EXECUTIVE VICE PRESIDENT

FROM: Alan MacMullin
Deputy Assistant Inspector General
for Finance and Pricing

SUBJECT: Audit Report – U.S. Postal Service's Implementation of Enterprise Risk Management (Report Number 21-235-R22)

This report presents the results of our audit of the U.S. Postal Service's Implementation of Enterprise Risk Management.

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

Attachment

cc: Corporate Audit Response Management
Postmaster General

Results

Introduction/Objective

This report presents the results of our self-initiated audit of the U.S. Postal Service implementation of the Enterprise Risk Management (ERM) Operating Charter (Charter) (Project Number 21-235). Our objective was to assess the effectiveness of the Postal Service's implementation of the Charter and identify opportunities to improve the ERM program. See Appendix A for additional information about this audit.

Background

The primary mission of the Postal Service's ERM program is to provide reasonable assurance that significant risks to and opportunity losses for the organization are systematically and effectively identified, evaluated, and mitigated where appropriate. The Postal Service based the program on the ERM framework published by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).[1] The Charter indicates that ERM efforts are led by Finance, as directed by the Chief Financial Officer (CFO) and the Vice President (VP), Controller. The Executive Leadership Team (ELT) in general and the CFO in particular, with oversight by the Postal Service Board of Governors' (Board) Audit and Finance Committee (AFC), work to:

- Ensure proper alignment of Postal Service targets for risk mitigation (risk appetite/tolerance),[2] strategy, and allocation of resources;
- Define responsibilities for risk management across the organization;
- Drive progress in meeting targets for risk management;
- Enhance risk response decisions; and
- Ensure regular reporting on efforts and results of ERM.

Management assesses the business environment and major enterprise risks as part of the Postal Service's strategic planning process. They develop strategic initiatives to achieve the Postal Service's long-term goals and address related enterprise risks that threaten progress toward those goals. Each initiative is sponsored by a member of the ELT. In addition, the Postal Service has corporate-wide efforts (for example, continuity of operations) and other efforts to address enterprise risks not related to the strategic planning process. Whether addressed through strategic initiatives or separate efforts, each enterprise risk is assigned a primary risk owner – nearly all of which are ELT members.

> *"There are no requirements for the Postal Service to have an ERM program."*

A biennial ERM survey of management across the organization is led by the VP, Controller, with a 20-member ERM Steering Committee playing a key role in reviewing risk ratings. The VP, Controller, briefs the ELT and AFC on the results of surveys and provides quarterly updates on the status of high risks. A two-person team supporting the ERM program (the ERM group) tracks the status of high risks quarterly and broadly monitors moderate and lower rated risks.

There are no requirements for the Postal Service to have an ERM program. Unlike most federal agencies, the Postal Service is not required to comply with the Office of Management and Budget's Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control,* July 2016. Further, the Postal Service's obligation to comply with certain U.S. Securities and Exchange Commission financial reporting requirements,[3] as well as generally accepted accounting principles, do not require an ERM program.

1 Committee of Sponsoring Organizations of the Treadway Commission, *Enterprise Risk Management – Integrating with Strategy and Performance,* June 2017.
2 Risk appetite means the type and amount of risk an organization is willing to accept in pursuit of its objectives. Risk appetite levels can vary from program to program as long as they fall within the risk appetite boundaries for the organization when consolidated. Risk tolerance refers to an acceptable range of variation in performance relative to a business unit or program objective and helps determine how performance aligns with the unit's risk appetite.
3 Public Law 109-435, Postal Accountability and Enhancement Act, Section 3654, Additional Financial Reporting, requires filing certain financial reports containing the information required by the SEC, with the Postal Regulatory Commission, as well as compliance with internal control reporting for the Sarbanes-Oxley Act of 2002.

Findings Summary

The Postal Service effectively implemented many provisions of the Charter. We found that ERM is integrated with the strategic planning process and the ERM program is aligned with the strategic goals and objectives published in the Postal Service's ten-year[4] and five-year strategic plans.[5] Also, management has been effective in driving progress on risk response plans, enhancing risk decisions, and providing regular reporting on ERM efforts to the AFC. However, we identified several elements of the Charter that were not fully implemented.

Additionally, we found that the Postal Service ERM program incorporated several approaches identified in federal and industry guidance as good ERM practices. For example, the Postal Service established a customized ERM program integrated into existing agency processes. We identified several additional opportunities for management's consideration to improve the Postal Service ERM program.

"While management effectively implemented multiple aspects of the Charter, we identified elements related to reviews, program targets, and responsibilities that they did not fully implement."

Finding #1: ERM Operating Charter Implementation

While management effectively implemented multiple aspects of the Charter, we identified elements related to reviews, program targets, and responsibilities that they did not fully implement. The Charter states it will be reviewed at least annually. The Charter also instructs the ELT and CFO to ensure proper alignment of Postal Service targets for risk mitigation, strategy, and allocation of resources, and to define responsibilities for risk management across the organization.

Specifically:

- Annual review – The current version of the Charter dates back to 2013. While the Charter should be reviewed at least annually, it does not specify who is responsible for performing annual reviews and management has not established a formal schedule for review. The ERM group stated that they recently reviewed the Charter and are preparing suggested revisions. Without annual reviews, the Charter may not reflect the current needs of the organization.
- Risk mitigation targets – Management has not set specific targets for risk mitigation; therefore the intention described in the Charter to align these with strategy and allocation of resource targets cannot be met.

  The Charter associates risk mitigation targets with risk appetite; however, management has not set a risk appetite for the organization as a whole or individually for any of the five risks we sampled. A defined risk appetite can inform risk owners' decisions on whether to accept, avoid, reduce, share, or transfer a risk. Without a clear definition, risk owners may accept more risk, or be more conservative than senior leaders intend, when developing their risk responses.
- Resource allocation targets – Management stated that they do not track ERM costs separately or budget for ERM. Similar to risk mitigation targets, if resource allocation targets are not identified, they cannot be aligned with targets for risk mitigation and strategy as intended by the Charter.
- Risk management responsibilities – Management confirmed that there is no policy or other documentation that defines ERM responsibilities across the organization. Management said some of the responsibilities could be embedded within officer role mandates. Managing risk is everyone's responsibility, but without defined ERM responsibilities it is not possible for employees at all levels of the organization to know their role in risk management.

4 United States Postal Service, Delivering for America, *Our Vision and Ten-Year Plan to Achieve Financial Sustainability and Service Excellence*, March 2021
5 Ready-Now —> Future Ready, *The U.S. Postal Service Five-Year Strategic Plan, FY 2020-FY 2024.*

Management stated that they were not in their current positions when the Charter was last updated, therefore, could not explain why these elements were not implemented. They stated it may have been because of a lack of resources. The ERM group consists of only two employees who perform ERM duties part-time in addition to numerous accounting responsibilities. We noted that at the time of our audit, the Postal Service had not updated the Charter in the prior eight years. As a result, the ERM program may not provide sufficient assurance that significant risks and opportunity losses to the Postal Service are systematically and effectively identified, evaluated, and mitigated as intended by the AFC. Such risks and losses could directly impact the financial position or ability to meet service goals, resulting in damage to the Postal Service's reputation and brand.

Recommendation #1

We recommend the **Chief Financial Officer and Executive Vice President** review and update the Enterprise Risk Management Operating Charter to reflect the current needs of the organization and implement the revised Charter.

Finding #2: Opportunities to Improve the ERM Program

The Postal Service ERM program incorporates several of the initial steps suggested by COSO for a successful ERM effort.[6] Management incorporated involvement by senior leaders, such as the AFC and ELT, established a leader to drive the ERM initiative, created the ERM Steering Committee, and implemented a process to identify and periodically rate enterprise risks.

COSO suggests other initial steps for a strong foundation and advises that it is important to maintain momentum to realize the full benefits of an ERM program. Several examples of these steps are also presented in federal ERM guidance by the U.S. Government Accountability Office (GAO)[7] and United States Chief Financial Officers Council and Performance Improvement Council.[8] We identified several opportunities for improving the Postal Service ERM program.

Identify and Inventory Existing Risk Management Practices

Identifying and cataloging existing ERM practices, whether formal or informal, can help management better ensure they are aligned and coordinated to identify risks related to the organization's primary goals. This will also allow management to identify gaps in policies and guidance as well as the lack of a common risk language. COSO advises on the importance of establishing a robust, consistent methodology and terminology for a successful ERM program. ERM practices presented for the Postal Service's consideration include:

- Document the structure of current ERM practices in policy and process documents. Other than the 2-page Charter discussed in Finding 1, management could not provide documentation of ERM policies or guidance provided to those with enterprise risk responsibilities. ERM documented policies can avoid being seen as standalone policy by referencing ERM-related aspects of existing planning, budget, or strategic processes. This would serve to further establish the relationship between ERM, strategy setting, and performance management.[1,7,8]
- Create a common risk language that describes the core concepts and terms that form the basis of the Postal Service ERM program. COSO states that a common risk language is necessary to communicate and establish consistent risk processes across an organization. A common risk language provides consistency in how program areas assess and report on risk, and share risk related information.[7,8]

> *"Identifying and cataloging existing ERM practices, whether formal or informal, can help management better ensure they are aligned and coordinated to identify risks related to the organization's primary goals."*

6 Committee of Sponsoring Organizations of the Treadway Commission, Creating and Protecting Value, Understanding and Implementing Enterprise Risk Management, January 2020.
7 *Enterprise Risk Management: Selected Agencies' Experiences Illustrate Good Practices in Managing Risk,* GAO-17-63, December 2016.
8 Chief Financial Officers Council and the Performance Improvement Council, Playbook: Enterprise Risk Management for the Federal Government, July 2016.

- Provide guidance for risk owners as they identify the appropriate response and goals within the business context, performance targets, and organization's risk appetite, for each risk. Guidance may include how to interpret and apply the various types of risk responses: accept, avoid, reduce, transfer, and share within their program areas. While goals, targets and metrics are set at the business initiative level, the risk owners or representatives of five sampled enterprise risks were not able to describe the risk appetite for the organization or for their program, from an enterprise risk management perspective, during our interviews with them.[7]
- Maintain records of ERM discussions and decisions such as those made by the ERM Steering Committee.[1,8]

Enhance Risk Reporting

COSO advises that a robust risk reporting process is necessary to respond to the dynamic nature of risks and ongoing changes to an organization's strategies. As risk management processes evolve, reporting can adjust to become more granular and detailed. Large and complex organizations may find the use of technology and quantitative metrics more useful in a robust ERM environment. Reporting enhancements presented for the Postal Service's consideration include:

- Expand ERM reporting to provide more specific data on how key risk responses are reducing risk to the organization or are otherwise successfully meeting risk response expectations. COSO advises that the real value of ERM is in developing action plans and managing identified risks. Management should identify and report when that value is realized by the organization.[1,8]
- Develop dashboards to more efficiently manage ERM program oversight.[7,8]
- Leverage existing strategic planning briefings to integrate information on the status of relevant enterprise risks into strategic initiative discussions with the ELT. Management from the Office of Strategic Planning said they do not currently discuss enterprise risks in their regular 'Get It Right' briefings on strategic initiatives. By integrating enterprise risks elements into these discussions, senior management can better assess whether risk responses are leading to reduced risks and supporting progress on the organization's key initiatives.[7]

Develop The Next Phase

When the initial ERM program has been established, COSO advises organizations to conduct a critical assessment of program accomplishments, such as benefits achieved to date, and develop the next steps in the evolution. A visual tool such as a strategy map depicting the organization's business objectives, strategies, risks, and risk management processes can provide management the opportunity to identify gaps in existing ERM activities. Such visualizations can also provide the AFC with a starting point for discussing the integration of ERM and strategic initiatives. Next phase elements presented for the Postal Service's consideration include:

"Large and complex organizations may find the use of technology and quantitative metrics more useful in a robust ERM environment."

- Articulate the goals and expected outcomes of oversight of the ERM program. These goals and outcomes should be defined within the context of the organization and could take a variety of forms. For example, if the goal is to establish an ERM dashboard, oversight outcomes could be measured by the proportion of enterprise risk response plans to defined key risk indicators that feed into the dashboard. With established goals, the organization could periodically assess its effectiveness and determine whether resources are sufficient to achieve the desired outcomes.[1,7]
- Ensure the Office of Strategic Planning is represented on the ERM Steering Committee for stronger collaboration on which enterprise risks are most directly impacting the organization's strategic plans and goals. Due to personnel changes the Office of Strategic Planning was not represented at the time of the audit. COSO advises that linking the impact of risks more closely to strategic initiatives enables the organization to focus on those risks most critical and worthy of time and attention.[1]

- Build organization wide communications to convey ERM's importance and relevance to daily operations. Currently, ERM communications primarily circulate within a limited audience made up of the ERM Group, ERM Steering Committee, ELT, and AFC. We noted that an employee searching for information about the Postal Service's ERM program would find very limited information, most of which is several years old and not specific to Postal Service operations. Elements of communication could include:
  - Providing training throughout the organization;
  - Providing specialized training for risk owner and risk response participants;[8]
  - Creating channels through which employees can raise risk concerns; and
  - Expanding stakeholder feedback.[7]

  COSO advises that education and communications concerning the role and objective of ERM are necessary. These communications should be straightforward, iterative, and widespread across the organization. They should articulate the priority that management places on ERM and how it impacts achieving the organization's mission and goals.[1,7,8]

  If adapted for the Postal Service environment, the practices discussed could enable the AFC to make better informed decisions and ultimately improve the organization's performance as it works to reach business objectives, meet its mission, and protect its brand.

Recommendation #2

We recommend the **Chief Financial Officer and Executive Vice President** consider the opportunities for improvement discussed in the report and identify actions to further develop the Enterprise Risk Management program.

Management's Comments

Management agreed with the findings and recommendations.

Management agreed to address both recommendations in conjunction with each other. They agreed to evaluate potential changes to the program and the biennial survey and update the charter accordingly. They will consider each of the suggested opportunities for improvement with awareness of resources needed and the added value to the ERM program and the organization as a whole. The target implementation date is February 28, 2023.

See Appendix B for management's comments in their entirety.

Evaluation of Management's Comments

The U.S. Postal Service Office of Inspector General (OIG) considers management's comments responsive to the recommendations and the corrective actions should resolve the issues identified in the report.

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.

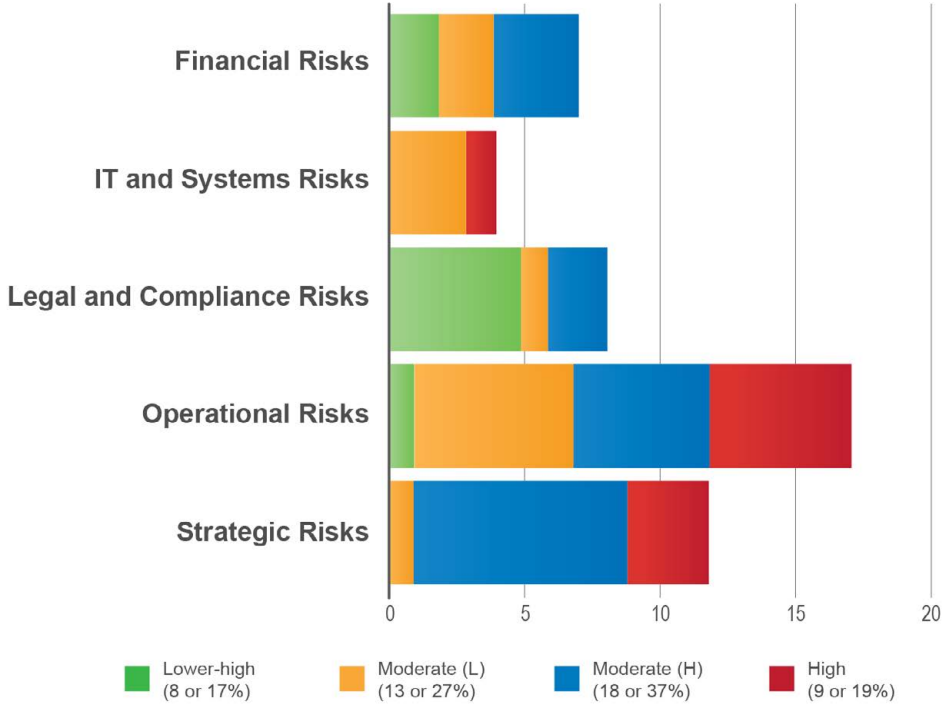
Appendix A: Additional Information

Scope and Methodology

The scope of the audit was the Postal Service's current ERM program. We excluded assessment of the risk management culture, the reasonableness of risk ratings, and the reliability of any software or systems used to identify, track, or manage enterprise risks. Further, we did not assess internal controls used to manage, mitigate, or monitor individual risks identified through the ERM program.

We selected a sample of five enterprise risks using the results of the Postal Service's FY 2021 ERM survey. Following analysis and minor adjustments, the FY 2021 ERM survey results reported ratings for 48 risks across five categories: financial, information technology (IT) and systems, legal and compliance, operational, and strategic as shown in Figure 1.

Figure 1. Distribution of FY 2021 ERM Risks Across Risk Categories



Source: OIG analysis of FY 2021 ERM survey results.

We structured our random sampling of enterprise risks to include new and pre-existing risks, risks from each risk category, from each ranking level (for example, High, Moderate (H), and risks where the response activities included and did not include strategic initiatives. Table 1 shows the enterprise risks sampled for this audit.

Table 1. Sampled Enterprise Risks

	Sampled Enterprise Risk	Risk Category	Risk Level	Risk Response Tied to Strategic Initiatives
1.	Bureaucracy	Strategic Risks	Moderate (High)	Yes
2.	Commodity	Financial Risks	Moderate (Low)	No
3.	Cyber Security	IT and Systems Risks	High	Yes
4.	Employee Availability*	Operational Risks	High	Yes
5.	Environment, Health, & Safety	Legal and Compliance Risks	Lower	Yes

Source: Postal Service FY 2021 ERM survey results and related Technology Management Office Software (TMOS) records. An asterisk (*) indicates the risk was newly included in the survey for FY 2021.

To accomplish our objectives, we:

- Interviewed personnel from the Office of the Controller with ERM program responsibilities, the Office of Strategic Planning, those with ownership of the five sampled enterprise risks, and the Office of the Board.
- Evaluated available ERM process documentation, communications, and reporting.
- Assessed how the ERM process is integrated into the organization's strategic planning process.

- Obtained results of the FY 2021 ERM survey.
- Reviewed the risk response activities involving monitoring and/or mitigation actions for a random sample of enterprise risks.
- Obtained and reviewed TMOS for records related to the risk responses for sampled risks.
- Assessed ERM processes, mitigation activities, monitoring efforts, and outcomes against the Charter and related policies to measure effectiveness.
- Compared ERM processes to federal and industry guidance to identify potential actions for enhancing and improving the ERM program.

The industry documents, good practices, and government-wide guidance used in our review included:

- COSO *Enterprise Risk Management – Integrating with Strategy and Performance,* June 2017.
- COSO *Creating and Protecting Value, Understanding and Implementing Enterprise Risk Management,* January 2020.
- Chief Financial Officers Council and the Performance Improvement Council *Playbook: Enterprise Risk Management for the Federal Government,* July 2016.
- GAO Report, *Enterprise Risk Management: Selected Agencies' Experiences Illustrate Good Practices in Managing Risk,* GAO-17-63, December 2016.
- North Carolina State, Poole College of Management, Enterprise Risk Management Initiative, *The State of Risk Oversight: An Overview of Enterprise Risk Management Practices,* April 2021.

We conducted this performance audit from October 2021 through May 2022 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 April 22, 2022, and included their comments where appropriate.

We did not assess the reliability of any computer-generated data for the purposes of this report because no such data was relevant to the audit objective.

Prior Audit Coverage

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

Appendix B: Management's Comments

JOSEPH CORBETT
CHIEF FINANCIAL OFFICER
EXECUTIVE VICE PRESIDENT

UNITED STATES POSTAL SERVICE

May 10, 2022

JOHN CIHOTA
DIRECTOR, AUDIT OPERATIONS

SUBJECT: U.S. Postal Service's Implementation of Enterprise Risk Management
Report Number 21-235

Thank you for the opportunity to respond to the OIG's report on our implementation of Enterprise Risk Management (ERM). As the OIG notes in their report, we have successfully implemented many aspects of the ERM operating charter and aligned our program with several best practices identified in our research of federal and industry ERM programs. Nonetheless, we continually look for ways to improve our program and appreciate the recommendations provided by the OIG.

Finding #1: ERM Operating Charter Implementation: We agree with the OIG's finding that identified elements related to annual reviews, program targets, and defined responsibilities within the ERM operating charter were not fully implemented.

Recommendation 1:
The OIG recommends the Chief Financial Officer and Executive Vice President review and update the Enterprise Risk Management Operating Charter to reflect the current needs of the organization and implement the revised Charter.

Management Response/Action Plan:
We agree with the OIG's recommendation and will update and implement the revised Charter. This recommendation works in conjunction with Recommendation 2. As we evaluate potential changes to the program and to our biennial survey, we will update the Charter accordingly. Thus, the timing for implementing Recommendation 1 coincides with the timing for implementing Recommendation 2.

Target Implementation Date:
February 2023

Responsible Official:
Assistant Controller

475 L'ENFANT PLAZA SW
WASHINGTON, DC 20260-5000
[redacted]
FAX: 202-268-4364
WWW.USPS.COM

Finding #2: Opportunities to Improve the ERM Program: We agree with the OIG's finding that opportunities exist to improve the ERM program.

Recommendation 2:
The OIG recommends the Chief Financial Officer and Executive Vice President consider the opportunities for improvement discussed in the report and identify actions to further develop the Enterprise Risk Management program.

Management Response/Action Plan:
We agree with the OIG's recommendation and will consider each of the suggested opportunities for improvement, being mindful of the resources needed to implement the suggestions and the added value to the ERM program and the organization as a whole.

Target Implementation Date:
February 2023

Responsible Official:
Assistant Controller

Joseph Corbett

cc: Manager, Corporate Audit Response Management

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

For media inquiries, please email
press@uspsoig.gov or call 703-248-2100