Office of Inspector General | United States Postal Service

Audit Report

# U.S. Postal Inspection Service's Online Analytical Support Activities

Report Number 21-191-R22 | March 25, 2022

# Table of Contents

# Highlights

## Background

The U.S. Postal Inspection Service's Analytics and Cybercrime Program provides investigative, forensic, and analytical support to field divisions and headquarters. A core component of this program is the Internet Covert Operations Program (iCOP), established in 2018 to provide analytics support for online investigations. Analysts respond to requests for assistance from postal inspectors and proactively gather intelligence using cryptocurrency analysis, open-source intelligence, and social media analysis. In April 2021, iCOP was renamed the Analytics Team.

## What We Did

This report responds to a request from the House of Representatives Committee on Oversight and Reform to evaluate the Postal Inspection Service's online analytical support activities, including its statutory authority and processes for these activities, and any related contracts. We reviewed 434 online analytical support requests from a statistical sample of 160 cases and 70 reports produced by iCOP to assess whether these activities were authorized. We also reviewed policies, procedures, and contracts associated with iCOP and the Analytics Team.

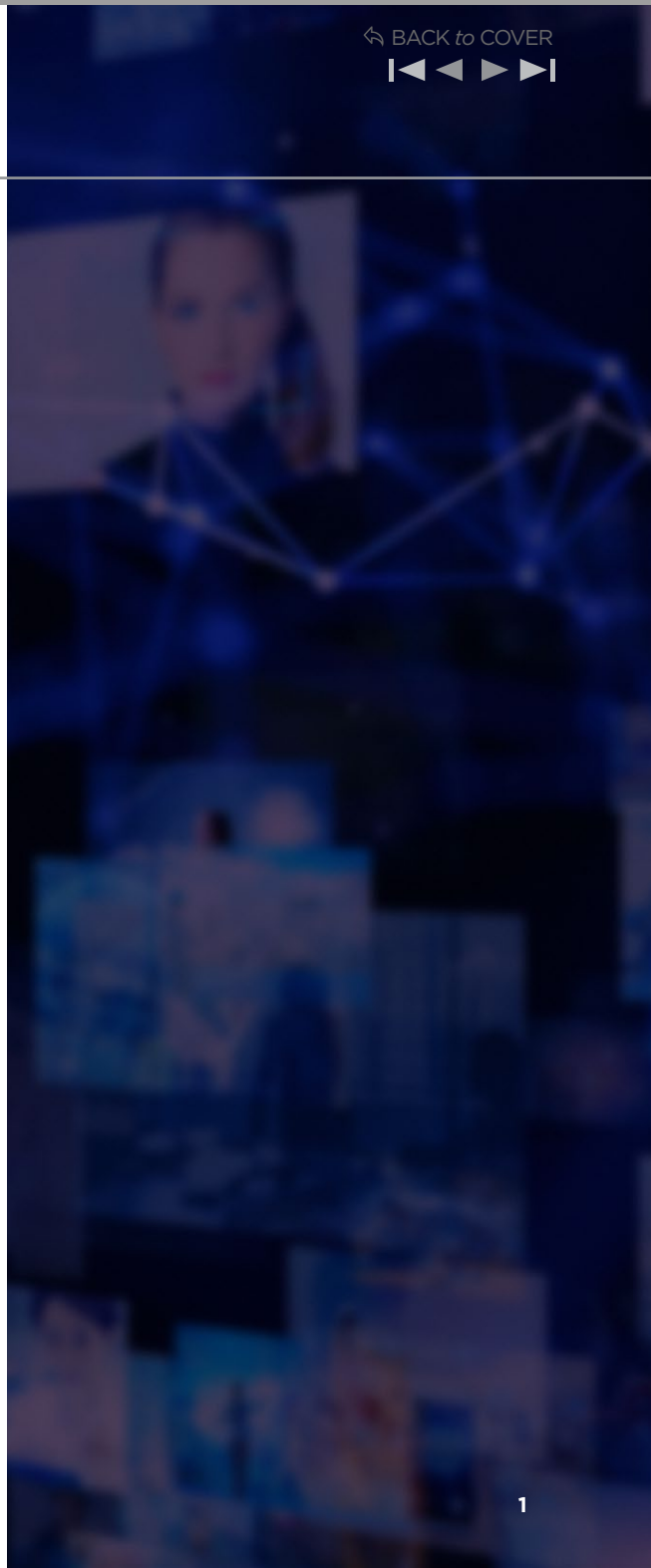
## What We Found

We determined that certain proactive searches iCOP conducted using an open-source intelligence tool from February to April 2021 exceeded the Postal Inspection Service's law enforcement authority. Furthermore, we could not corroborate whether other work analysts completed from October 2018 through June 2021 was legally authorized. The Postal Inspection Service's activities must have an identified connection to the mail, postal crimes, or the security of Postal Service facilities or personnel (postal nexus) prior to commencing. However, the keywords used for iCOP in the proactive searches did not include any terms with a postal nexus. Further, the postal nexus was not documented in 122 requests and 18 reports due to a lack of requirements in the program's procedures. These issues occurred because management did not involve the Postal Inspection Service's Office of Counsel in developing iCOP or its procedures.

We also found that iCOP did not develop a records management policy or sensitive information storage and retention standards. As a result, analysts did not retain information needed to ensure compliance with the Postal Inspection Service's legal authority. Finally, contracts supporting these activities did not include all required documents upon award, but management resolved this deficiency when we brought it to their attention.

## Recommendations

We are making six recommendations, including that management conduct a full review of the Analytics Team to ensure activities are authorized; revise the Analytics Team's Standard Operating Procedures; and develop storage and retention policies.



# Transmittal Letter

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

March 25, 2022

**MEMORANDUM FOR:** GARY R. BARKSDALE
CHIEF POSTAL INSPECTOR

CRAIG I. GOLDBERG
DEPUTY CHIEF INSPECTOR, HEADQUARTERS

LOUIS J. DIRIENZO
CHIEF COUNSEL, U.S. POSTAL INSPECTION SERVICE

THOMAS J. MARSHALL
GENERAL COUNSEL AND EXECUTIVE VICE PRESIDENT

Margaret B. McDavid

**FROM:** Margaret B. McDavid
Deputy Assistant Inspector General for Deputy Assistant Inspector General, Inspection Service, Cybersecurity and Technology

**SUBJECT:** Audit Report – U.S. Postal Inspection Service's Online Analytical Support Activities (Report Number 21-191-R22)

This report presents the results of our audit of the U.S. Postal Inspection Service's Online Analytical Support Activities.

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

Attachment

cc: Corporate Audit Response Management
Postmaster General

# Results

## Introduction/Objective

This report presents the results of our audit of the U.S. Postal Inspection Service's Online Analytical Support Activities (Project Number 21-191). The report responds to a request from Carolyn B. Maloney, Chairwoman, and James Comer, Ranking Member, on behalf of the House of Representatives Committee on Oversight and Reform. Our objective was to evaluate the Postal Inspection Service's online analytical support activities, including its statutory authority and processes for these activities, and any related contracts. See Appendix A for additional information about this audit.

## Background

The mission of the Postal Inspection Service is to support and protect the U.S. Postal Service and its employees, infrastructure, and customers; enforce the laws that defend the nation's mail system from illegal or dangerous use; and ensure public trust in the mail. Postal inspectors are federal law enforcement agents authorized to carry out this mission. Specifically, postal inspectors are authorized to investigate criminal matters related to the Postal Service and the mails, including all allegations of violations of postal laws or misconduct by individuals other than postal employees. Their law enforcement powers are limited to postal offenses, and can be expanded to other laws pursuant to agreement between the Attorney General and the Postal Service.[1]

> *"The Internet Covert Operations Program (iCOP) was established in 2018 to provide analytics support for online investigations."*

The Postal Inspection Service's Analytics and Cybercrime Program[2] provides investigative, forensic, and analytical support to field divisions and headquarters. A core component of the Analytics and Cybercrime Program was the Dark Web Program, which provided postal inspectors with open source and dark web intelligence, cryptocurrency management, online undercover methods and tools, and dark web and online undercover training. In October 2018, the Dark Web Program was renamed the Internet Covert Operations Program (iCOP) and expanded to provide support for all online covert operations. iCOP also began providing other analytical support, including facial recognition and social media monitoring services. On April 28, 2021, the Postal Inspection Service announced internally that the group of analysts responsible for these online analytical support activities would be referred to as the Analytics Team. The Analytics Team is comprised of two senior analysts and six contracted analysts.

According to the Analytics Team's Standard Operating Procedures (procedures),[3] their mission is to:

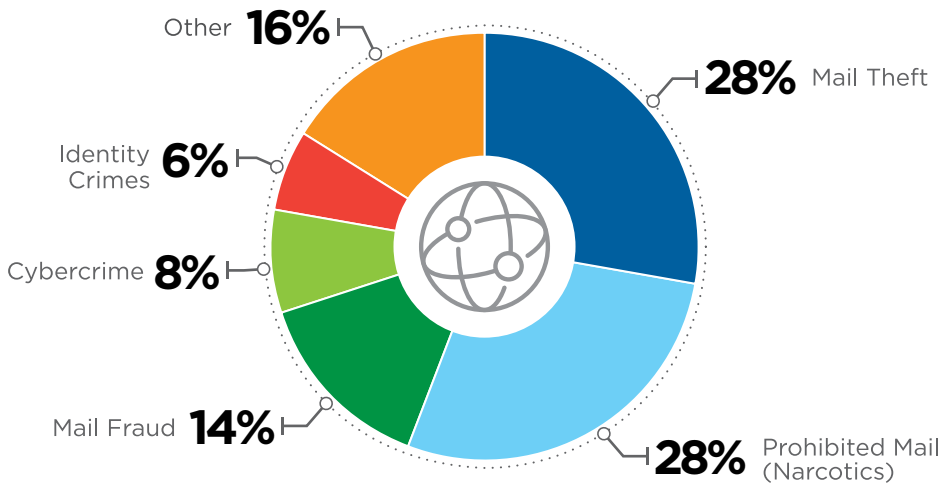
- Identify and develop intelligence on targets operating on the clear and dark webs[4] for all Inspection Service investigations.
- Provide actionable intelligence through cryptocurrency tracking and analysis, open-source intelligence and social media analysis, geospatial mapping and data visualization, and Postal Service backend and network data exploitation.
- Engage in proactive threat hunting and targeting intelligence to support each Inspection Service Program area as well as threats to Postal Service executives, employees, infrastructure, and facilities.
- Provide dedicated support for local and national critical incidents in support of field division operations.

1 18 United States Code §3061(a) and (b) and 39 Code of Federal Regulations §233.1.
2 In February 2022, the Postal Inspection Service split this program into two areas: (1) Analytics and (2) Cyber and National Security. Online analytical support activities are carried out under the Analytics Program.
3 Analytics Team Standard Operating Procedures, Postal Inspection Service Cybercrime & Analytics Program Analytics Team, Version 2.9, Revised May 10, 2021.
4 The clear web refers to the region of the internet most people are familiar with, including publicly accessible web pages indexed on search engines. The dark web is an intentionally concealed internet location that is only accessible to users who download special software that anonymizes their computers' location.

*"From October 2018 through March 2021, more than half of the 1,745 work assignments completed by iCOP or the Analytics Team fell into one of two program areas – Prohibited Mail-Narcotics and Mail Theft."*

From October 2018 through March 2021, more than half of the 1,745 work assignments completed by iCOP or the Analytics Team fell into one of two program areas – Prohibited Mail-Narcotics and Mail Theft. Figure 1 shows the distribution of work completed by program area.

**Figure 1. Percentage of iCOP Work Completed by Program Area**




Source: U.S. Postal Inspection Service.
Note: "Other" includes 18 other program areas, such as Workplace Violence, Prohibited Mail-Firearms, and Anti-Money Laundering.

According to management, a majority of analysts' work is done in response to a request for assistance from a postal inspector. The information that analysts produce varies depending on postal inspector investigative needs, but it can include raw output from a variety of tools the Analytics Team uses to conduct manual and automated searches. Table 1 describes some of these tools.

**Table 1. Select Tools Used by The Postal Inspection Service**

| Tool | Purpose |
|---|---|
| [redacted] | Provides cryptocurrency blockchain analysis |
| [redacted] | Provides detailed background information about individuals |
| [redacted] | Searches for unidentified suspects from images using facial recognition |
| [redacted] | Searches social media for open-source information about individuals |
| [redacted] | Manages proactive intelligence gathering searches by monitoring open-source websites for predefined sets of keywords |

Source: U.S. Postal Service Office of Inspector General (OIG) review of Postal Inspection Service documents.

Analysts may also create several types of reports based on their research for a postal inspector or proactive work. The report types are:

- **Intelligence Analysis Report:** Provides the reader with in-depth analysis of a moniker, activity, threat, or technical assessment and is generally issued in response to a request from an inspector.
- **Threat Assessment:** Provides the reader with quick updates or intelligence during an active situation involving a specific critical incident.
- **Situational Awareness Bulletin:** Provides the reader with information on a general topic or specific event and is designed for intelligence awareness and briefing.

According to management, a majority of the reports iCOP analysts produce support postal inspector investigations, but analysts also produce reports that assess threats unrelated to specific investigations. Depending on the intelligence

related to these threats, the reports may be disseminated to agencies outside of the Postal Inspection Service.

## Findings Summary

We determined that certain proactive searches iCOP conducted using an open-source intelligence tool from February to April 2021 exceeded the Postal Inspection Service's law enforcement authority. Furthermore, we could not corroborate whether other work analysts completed from October 2018 through June 2021 was legally authorized. We also found that management did not develop a records management policy or sensitive information storage and retention standards for iCOP. Finally, contracts supporting these activities did not include all required documents upon award.

## Finding #1: Authorization for Online Analytical Support Activities

We determined that, from February 19 to April 21, 2021, certain proactive intelligence searches that iCOP conducted using an open-source intelligence tool exceeded the Postal Inspection Service's law enforcement authority. Furthermore, we could not corroborate whether 28 percent of the work iCOP and Analytics Team analysts completed from October 2018 through June 2021 was authorized under the Postal Inspection Service's legal authority. Title 18 U.S.C. §3061(a) and (b) and 39 CFR. §233.1 authorize postal inspectors to investigate criminal matters related to the Postal Service and the mails and enforce laws regarding property in the custody of the Postal Service, property of the Postal Service, the use of the mails, and other postal offenses.[5] For analysts' activities to be authorized, their work must have an identified postal nexus prior to commencing.

*"For analysts' activities to be authorized, their work must have an identified postal nexus prior to commencing. This nexus should be a connection to the mail, postal crimes, or the security of Postal Service facilities or personnel."*

This nexus should be a connection to the mail, postal crimes, or the security of Postal Service facilities or personnel. According to management, the postal nexus would likely be identified in the requests for assistance that postal inspectors send to the analysts, though such requests are not used for proactive work.

### Proactive Intelligence Searches

From February 19 to April 21, 2021, iCOP used one of the 10 profiles established in the [redacted] intelligence tool to conduct searches that were not legally authorized. This tool manages proactive intelligence gathering by constantly monitoring open-source websites, including social media and message platforms, for predefined sets of keywords. The keywords iCOP used for one of the [redacted] profiles during this time did not include any terms related to the mail, postal crimes, or security of postal facilities or personnel. Examples of the keywords include "protest," "attack," and "destroy." According to the program manager, iCOP intentionally omitted terms that would indicate a postal nexus in an effort to broadly identify threats that could then be assessed for any postal nexus.

*"From February 19 to April 21, 2021, iCOP used one of the 10 profiles established in the [redacted] intelligence tool to conduct searches that were not legally authorized."*

After these keywords were removed, the iCOP program manager sent the remaining keywords for all of the [redacted] profiles to the Postal Inspection Service's Office of Counsel for review. On April 30, 2021, an Office of Counsel attorney recommended the term "protest" be removed from another profile to protect people's constitutional rights.

According to the Office of Counsel, this review was a part of their effort to better ensure that keywords used for proactive intelligence searches have a clear postal nexus and are authorized. While the Office of Counsel began requiring the Analytics Team to submit [redacted] keyword additions for approval, there was no requirement that the Office of Counsel review revisions or deletions of current

5 39 CFR §233.1 also authorizes postal inspectors to investigate all allegations of violations of postal laws or misconduct by persons except for postal employees.

search terms, which could also affect the postal nexus of searches. According to management, the Office of Counsel began reviewing all [redacted] keyword changes, including deletions, in January 2022. However, the requirement for these reviews has not yet been incorporated into the program's procedures.

## Requests for Assistance

We reviewed 434 requests for assistance associated with a statistical sample of area and jacketed cases[6] that used the online analytical support services and could not corroborate that the work associated with 122 (28 percent) of these requests was authorized under the Postal Inspection Service's legal authority. For analysts' activities to be authorized, their work must have an identified postal nexus prior to commencing. The majority of the requests (72 percent) we reviewed identified a postal nexus in the information provided by the inspector.

> *"The majority of the requests (72 percent) we reviewed identified a postal nexus in the information provided by the inspector."*

Of the 122 requests that did not identify a postal nexus, 120 (98 percent) were associated with area cases. These requests sometimes contained very little or no explanation for the request. For example, 14 requests for facial recognition services contained no entries in either the assistance requested field or the investigation description field. Management provided reasonable explanations of the postal nexus from the responsible postal inspector for 113 of the 120 requests associated with area cases, but did not provide documentation to support the explanations. For seven of the requests, management either did not provide a reasonable explanation of a postal nexus or was unable to provide further information about the reason for the request because the Postal Inspection Service no longer employed the responsible postal inspector.

The remaining two requests that did not contain evidence of a postal nexus were associated with a jacketed case. According to management, the case was jacketed to investigate a lead identified from other ongoing cases. However, the case description specifically stated that the mail nexus was unknown at the time of case jacketing and management could not provide evidence that a mail nexus was identified before the case was closed.

## Reports

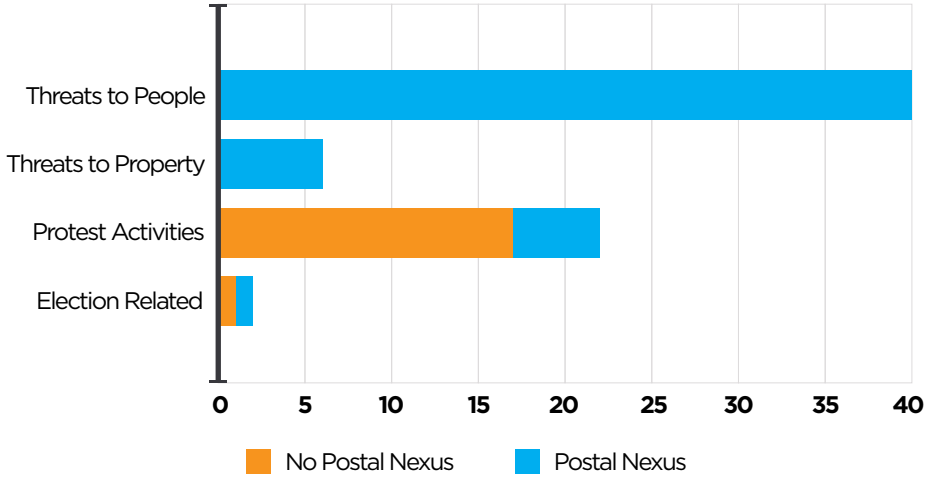
We also reviewed 70 reports produced by iCOP that assessed threats unrelated to specific investigations and determined that 18 (26 percent) did not identify a postal nexus within the report. These reports were produced from September 2020 to April 2021 and almost all (17 of 18) were associated with protest activities.[7] The focus of the reports ranged from summarizing potential protest activities nationwide to identifying activities in a specific location, but none identified how the potential protest activities related to the mail, postal crimes, or security of postal facilities or employees. In contrast, other reports we reviewed on the same topic identified a specific postal nexus, such as the number and proximity of postal facilities to a potential protest location.

The majority of the reports we reviewed (52 of 70, or 74 percent) identified a clear postal nexus and discussed specific threats to people, such as the Postmaster General, or property, such as a postal facility. Figure 2 identifies the breakdown of reports by topic and whether they identified a clear postal nexus.

6 The sample contained 160 open and closed cases. The Postal Inspection Service has a variety of case types. Area cases are used for preliminary investigative activities in broad program areas. Jacketed cases refer to investigations of specific criminal activity.

7 The remaining report was related to the 2020 election.

**Figure 2. iCOP Reports by Topic and Postal Nexus**




Source: OIG analysis of Postal Inspection Service reports.

According to management, the 18 reports that did not identify a clear postal nexus were all associated with officer, employee, or facility safety. However, we could not corroborate that this postal nexus was known prior to the start of the analysts' work, because analysts produced all 18 reports as part of their proactive threat hunting and targeting intelligence efforts, rather than in response to a specific request for assistance from a postal inspector. According to management, they task analysts with proactive work as needed, but do not track these assignments in any specific way. Once a report is produced, management will assign a tracking number, but this does not capture information about the original assignment. Further, as discussed in Finding #2, analysts do not retain any information related to their proactive work other than what is included in a final report. As a result, we could not confirm whether the work associated with these reports was authorized.

We found that the iCOP and Analytics Team procedures lack guidance related to online analytical support activities. Specifically, the procedures do not:

- Require approval of keywords used for proactive intelligence searches.
- Specify what information postal inspectors are required to submit with their requests.
- Require that proactive work assignments be documented or approved at the time work is initiated.
- Require reports to identify the postal nexus.

These issues occurred because management did not involve the Office of Counsel in the development or modification of iCOP or any of the related procedures. As a result, the program was developed without due consideration of the need to ensure all online analytical support activities undertaken by analysts can be clearly documented as being within the legal authority of the Postal Inspection Service. Additionally, without such documentation, we cannot determine the full extent to which the Postal Inspection Service has been collecting data about members of the public via open-source intelligence gathering.

According to the Office of Counsel, some efforts have been taken to improve internal controls related to the Analytics Team and the Postal Inspection Service's online analytical support activities. As discussed previously, the Office of Counsel began reviewing [redacted] search terms but has not yet documented this requirement in the program's procedures. Additionally, the Office of Counsel will now approve any reports that will be disseminated outside of the Postal Inspection Service to ensure the postal nexus is clear.

However, these efforts do not address larger concerns about the program. For example, national media coverage of a report produced by iCOP raised concerns among the public and congressional leaders about the Postal Service's activities.[8] Taking additional steps to conduct a comprehensive review of the Analytics Team's responsibilities, activities, and procedures will ensure that the Postal Inspection Service is operating within its jurisdiction and minimize additional reputational damage to the Postal Service.

8 *The Postal Service is Running a 'Covert Operations Program' that Monitors Americans' Social Media Posts*, Yahoo!News, April 21, 2021.

**Recommendation #1**
We recommend the **Postal Inspection Service's Chief Counsel**, in conjunction with the **Postal Service Law Department**, conduct a full review of the Analytics Team's responsibilities, activities, procedures, and any other associated guidance; and develop a process to ensure that all online analytical support activities conducted by the Postal Inspection Service are authorized.

**Recommendation #2**
We recommend the **Inspector-in-Charge, Analytics**, in consultation with the **Postal Inspection Service's Chief Counsel**, modify the Analytics Team's Standard Operating Procedures to require the Office of Counsel to document its approval of all predefined keywords used for proactive intelligence searches, including approval for any changes to the predefined keywords.

**Recommendation #3**
We recommend the **Inspector-in-Charge, Analytics**, in consultation with the **Postal Inspection Service's Chief Counsel**, modify the Analytics Team's Standard Operating Procedures to clarify documentation requirements for Requests for Assistance, to include requiring postal inspectors to document the postal nexus in their requests.

**Recommendation #4**
We recommend the **Inspector-in-Charge, Analytics**, in consultation with the **Postal Inspection Service's Chief Counsel**, modify the Analytics Team's Standard Operating Procedures to require the Office of Counsel to document its approval of proactive work assignments at the time they are initiated.

**Recommendation #5**
We recommend the **Inspector-in-Charge, Analytics**, in consultation with the **Postal Inspection Service's Chief Counsel**, modify the Analytics Team's Standard Operating Procedures to require that all reports identify the postal nexus.

## Finding #2: Records Retention and Storage of Sensitive Information

We determined that the Postal Inspection Service did not properly maintain records associated with online analytical support activities. Specifically, analysts stored sensitive information on their work computers and did not document how they used the information to respond to requests for assistance or develop reports.[9] This information frequently contained significant amounts of PII obtained from public sources, such as social media, and from contracted investigative tools that provide detailed background information such as addresses, birthdates, and social security numbers. According to analysts and management, after a report was completed, the only information retained on the analysts' computers was the information that could be found in the final report, along with the final and draft versions of the reports.

*"We determined that the Postal Inspection Service did not properly maintain records associated with online analytical support activities."*

The Postal Inspection Service maintains a task management database,[10] which is a controlled system accessible to analysts, postal inspectors, and management. Analysts use this system to receive and respond to postal inspector requests for assistance. However, according to analysts and management, only final intelligence products or reports are stored in this system. Therefore, it does not contain any interim information analysts may have gathered in response to postal inspector requests, or any information related to why or how analysts performed proactive work, such as initial search terms. Several of the intelligence tools include audit capabilities that allow the program manager to review analysts' search histories and results. However, these capabilities do not provide insight into what analysts do with the results.

9 According to Handbook AS-805, *Information Security*, sensitive information includes, but is not limited to, private information about individuals including marital status, age, or race. Sensitive-enhanced information includes, but is not limited to, law enforcement information and personally identifiable information (PII), which includes name and Social Security number.
10 This database is called [redacted] used to manage tasks and request assistance accessed via the Postal Inspection Service intranet.

According to Postal Service policy, management should set standards to ensure that records relevant for investigations are appropriately preserved and reasonably accessible.[11] Sensitive information should also be stored in a controlled area in accordance with established Postal Service policies and procedures.[12] However, Postal Inspection Service management did not establish a records management policy or sensitive information storage and retention standards for iCOP or the Analytics Team.

Without records related to analysts' interim intelligence gathering activities or proactive work, management lacks access to information needed to ensure compliance with the Postal Inspection Service's legal authority, such as the assignments and initial search terms used to produce the 18 reports discussed in Finding #1. Further, without proper storage of sensitive source materials, management cannot effectively assess the accuracy of the intelligence products produced by analysts or ensure that the information is adequately protected.

### Recommendation #6

We recommend the **Inspector-in-Charge, Analytics**, develop procedures for retaining documentation associated with work completed by the Analytics Team and storing sensitive information to ensure compliance with Postal Service policy.

## Finding #3: Contract Management

We found that the Contracting Officer did not prepare Contracting Officer Representative (COR) letters of appointment in a timely manner for two of the seven contracts awarded for products or services used by iCOP.[13] Postal Service policy states that COR duties and responsibilities are delineated in the letter of appointment and a copy of the notice of appointment defining the COR's authority is furnished to the supplier upon award of the contract.[14] The COR is responsible for the day-to-day administration of the contract and serves as the Postal Service's point of contact with the supplier on all routine matters. Failing to provide a letter of appointment can, therefore, result in a lapse of contract management, increasing the risk of contract-related fraud, waste, or abuse. The Contracting Officer signed both letters on September 28, 2021, after we brought the missing letters to the attention of Supply Management and the Postal Inspection Service. Therefore, we are not making a recommendation on this issue.

The Postal Service's Supply Management group has awarded seven contracts totaling almost $12 million to six suppliers for products or services used by iCOP, as well as postal inspectors in the field. These contracts are for various tools and analytical personnel services, as described in Table 2.

**Table 2. Contracts Awarded for Online Analytical Support**

| Supplier | Product or Service Description | Date Awarded | Period of Performance | Total Contract Value (as of January 2022) |
|---|---|---|---|---|
| [redacted] | Provides cryptocurrency blockchain analysis | 9/27/17 | 10/1/17–10/21/22 | $1,140,382 |
| [redacted] | Provides the location and identification of Internet Protocol addresses | 3/31/20 | 4/1/20–3/31/22 | $629,760 |
| [redacted] | Provides investigative analyst personnel | 10/11/19 | 10/1/19–9/30/22 | $4,729,920 |

11 Handbook AS-353, *Guide to Privacy, the Freedom of Information Act, and Records Management*, Section 6, Records Management, dated February 2019.
12 Handbook AS-805, *Information Security*, Section 3-5.3, Retention and Storage of Information, dated June 2021.
13 Letters for the contract awarded to [redacted] on September 27, 2017 and the contract awarded to [redacted] for [redacted] on February 23, 2021 were missing.
14 U.S. Postal Service *Supplying Principles & Practices* (SP&P), dated June 20, 2020. The SP&P are guidelines that the Postal Service follows when completing contracts.

| Supplier | Product or Service Description | Date Awarded | Period of Performance | Total Contract Value (as of January 2022) |
|---|---|---|---|---|
| [redacted] | [redacted]: Searches for unidentified suspects from images using facial recognition | 9/24/20 | 10/1/20–9/30/22 | $226,800 |
| | [redacted] Manages proactive intelligence gathering searches by monitoring open-source websites for predefined keywords | 2/23/21 | 2/23/21–2/22/22 | $118,647 |
| [redacted] | [redacted] Virtual machine platform to access Postal Inspection Service networked computers | 9/28/18 | 9/28/18–9/30/22 | $3,247,943 |
| [redacted] | Searches social media for open-source information about individuals | 9/13/19 | 10/1/19–9/30/22 | $1,820,160 |
| **Total** | | | | **$11,913,611[a]** |

Source: OIG analysis of Contract Authoring and Management System data and contract documents.
[a] Total may not add due to rounding.

## Management's Comments

Management disagreed with findings 1 and 2 and agreed with finding 3. Management agreed with recommendation 1; partially agreed with recommendations 2 and 6; and disagreed with recommendations 3, 4, and 5.

Regarding finding 1, management did not agree that certain proactive intelligence searches that iCOP conducted exceeded the Postal Inspection Service's law enforcement authority. Specifically, while they agreed that Postal Inspection Service activities need a postal nexus, they did not agree that the agency is required to limit searches to terms that have a postal nexus. Instead, they stated the focus should be on whether the purpose of the search itself has a postal nexus. Management stated that every search the Postal Inspection Service conducted, and the OIG reviewed, had a postal nexus.

Additionally, management stated that the program operates in compliance with existing policy, which does not require postal inspectors to document the postal nexus in their request for assistance prior to any work commencing. Management disagreed that documenting the postal nexus in a request is necessary because requests require a case number. Management stated the case number is confirmation that a postal nexus exists since a nexus is required when a case is opened.

Regarding recommendation 1, management agreed to conduct a full review of the Analytics Team's responsibilities, activities, procedures, and other associated guidance; and to develop a process to ensure that all online analytical support activities the Postal Inspection Service conducts are authorized. The target implementation date is September 30, 2022.

Regarding recommendation 2, management agreed to update the Standard Operating Procedures to clarify that keywords used to conduct pre-defined automated search activities will require Office of Counsel review and approval prior to being established or changed. In subsequent correspondence, management provided a target implementation date of April 29, 2022.

Regarding recommendations 3, 4, and 5, management did not agree to modify the Standard Operating Procedures. However, they agreed to adjust the procedures, as necessary, upon completion of the full review of the Analytics Team conducted in response to recommendation 1.

Regarding finding 2, management disagreed that the Postal Inspection Service did not properly maintain records associated with online analytical support activities. Specifically, they stated that the Postal Service is prohibited from collecting or maintaining records describing or relating to how an individual exercises his or her rights under the First Amendment, except where the record is pertinent to and within the scope of an authorized law enforcement activity.

Regarding recommendation 6, management did not agree to develop procedures for retaining documentation or storing sensitive information because they stated that the Analytics Team complies with current Postal Service policies regarding the storage of sensitive information. However, management agreed to adjust the procedures, as necessary, upon completion of the full review of the Analytics Team conducted in response to recommendation 1.

Regarding finding 3, management agreed that the finding has already been rectified but stated that the OIG inaccurately attributed the contract costs presented in Table 2 to the iCOP program.

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

## Evaluation of Management's Comments

Although there is significant disagreement documented in management's response to this report, the actions they agreed to take may fully address the recommendations. We will keep the recommendations open until the initial review of the online analytical support activities and procedures is conducted and changes are made. At that time, we will address any remaining recommendations in the audit resolution process, as appropriate. Therefore, the OIG considers management's comments generally responsive to the recommendations in the report.

Regarding finding 1, management stated that the postal nexus must relate to the purpose of the search and not to the keywords used. As noted in the report, the Postal Inspection Service does not document the purpose of proactive intelligence gathering assignments in any specific way. Further, automated proactive intelligence searches, such as those conducted through [redacted] only consist of keywords. Without information about why the keyword search profile was developed or a direct postal nexus in the keywords, there is no evidence to support management's claim that the Postal Inspection Service was within its law enforcement authority in carrying out these automated searches.

Further, although management stated that all requests have a postal nexus because they are associated with a case number, this does not provide adequate evidence to ensure that analysts' work is legally authorized. As we noted in this report, almost all of the requests that did not have a postal nexus were associated with area cases, which are used for preliminary investigative activities in broad program areas. Information gathered through area cases is used to develop a postal nexus and justify jacketing a case. Further, case jacketing does not always ensure that there is a postal nexus. We found two requests associated with a jacketed case that stated the mail nexus was unknown at the time of case jacketing. While current policy does not require postal inspectors to document the postal nexus in their requests, doing so will ensure that all online analytical support activities undertaken by analysts in response to requests are clearly within the legal authority of the Postal Inspection Service.

Regarding recommendation 3, we found that inspectors included an explanation of a postal nexus in 312 of the 434 requests that we reviewed, despite no policy requirement for them to do so. Therefore, we do not agree with management that such a requirement for all requests would be unnecessarily redundant.

Regarding recommendation 4, management repeatedly told us during our review that they do not document proactive intelligence gathering assignments in any specific way. Further, as stated in our report, current procedures and policies do not require that proactive work assignments be documented or approved at the time work is initiated.

Regarding recommendation 5, because analysts do not retain any information except that which can be found in the final report, there is no evidence that the work associated with these reports was authorized. Identifying the specific postal nexus in reports will ensure that the Postal Inspection Service is operating within its jurisdiction and minimize reputational damage to the Postal Service.

For recommendations 3, 4, and 5, management agreed to adjust the procedures, as necessary, upon completion of the full review of the Analytics Team conducted in response to recommendation 1. These recommendations will remain open.

Regarding finding 2, management contends that the Inspection Service was conducting authorized law enforcement activity when it conducted searches in response to postal inspectors' requests and proactive intelligence gathering, as described in finding 1. If this were the case, the First Amendment prohibition management cites in their response would not apply and such information should have been retained.

Regarding recommendation 6, management and the analysts repeatedly told us during our review that they did not have a records management policy or sensitive information storage and retention standards for their online analytical support activities. As discussed in the report, without such requirements, management lacks access to information needed to ensure compliance with the Postal Inspection Service's legal authority. Because management agreed to adjust the procedures, as necessary, upon completion of the full review of the Analytics Team conducted in response to recommendation 1, this recommendation will remain open.

Regarding finding 3, we revised the title of Table 2 to better reflect that postal inspectors also use these products and services in the field. While management stated that the agency as a whole uses these products and services, the program manager for the Analytics Team is the COR for all seven contracts.

All recommendations require OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective action(s) 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 our audit included a review of work completed by iCOP or the Analytics Team during the period October 1, 2018, to June 30, 2021. We also reviewed contracts used to support the program.

To accomplish our objective, we:

- Reviewed policies and procedures pertaining to the management of the program.
- Interviewed relevant officials including the Inspector in Charge and Assistant Inspector in Charge of the Analytics and Cybercrime Group, the iCOP or Analytics Team Program Manager and analysts, and officials in the Office of Counsel to gain an understanding of their roles and responsibilities as it relates to the program.
- Identified a statistical sample of 160 cases from the universe of 692 open and closed cases that used online analytical support services during our audit scope. We requested and reviewed 434 requests for investigative assistance made to the iCOP or Analytics Team related to the case sample.
- Reviewed 70 reports produced to assess threats unrelated to specific investigations to gain an understanding of the work iCOP conducted outside of investigative support.
- Reviewed seven contracts and related documentation awarded to support iCOP.
- Interviewed the Contracting Officer and COR to understand their process for providing oversight and management of the contracts.

We conducted this performance audit from June 2021 through March 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 February 17, 2022, and included their comments where appropriate.

We assessed the data reliability of the sampled cases by searching the cases in the Case Management System[15] and verifying that the information matched the system. We assessed the data reliability of the requests for assistance associated with the sampled cases by verifying that some of the data fields matched in the Case Management System and examining the completeness and reasonableness of other data fields. We also assessed contract data from the Contract Authoring and Management System[16] by comparing the information to documents provided by the Postal Inspection Service and Contracting Officers. 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 related to the objective of this audit within the last five years.

15 Postal Inspection Service database that documents and tracks case activities.
16 Postal Service system that houses contract information.

# Appendix B: Management's Comments

UNITED STATES POSTAL SERVICE

March 16, 2022

JOHN CIHOTA
DIRECTOR, AUDIT OPERATIONS

SUBJECT: U.S. Postal Inspection Service's Online Analytical Support Activities (Project Number 21-191-DRAFT)

**U.S. Postal Inspection Service Response**

**SUMMARY**

After conducting a thorough review of the U.S. Postal Service - Office of the Inspector General (USPS-OIG) audit report, we strongly disagree with the overarching conclusion that the U.S. Postal Inspection Service (Inspection Service) exceeded its authority and conducted improper intelligence searches. This response will address those main issues, as well as a number of other incorrect findings contained in the USPS-OIG audit report.

The Inspection Service is a federal law enforcement agency with broad authority to investigate offenses related to the U.S. Mail and U.S. Postal Service (Postal Service) employees, customers, and property. In addition to conducting criminal investigations, the Inspection Service is also responsible for protection of the mails, plant and personnel security, and coordinating Postal Service emergency preparedness planning. To accomplish these goals, case law and federal statutes permit the Inspection Service, like other law enforcement agencies, to use a wide variety of tools when conducting activities in furtherance of its mission. One such tool used by the Inspection Service is open-source intelligence (OSINT), which is willingly shared, publicly available information. When performing OSINT research to further its mission, the Inspection Service is authorized by federal law, as clearly supported in case law, to research a wide range of topics extending to conduct that could reasonably be said to impact or impair the proper operation of the Postal Service, or that in other words have a nexus to the Postal Service. We therefore assert that every search conducted by the agency, and reviewed by the USPS-OIG, had a postal nexus. The USPS-OIG's findings that the Inspection Service must only use postal terms to search open-source information is an unsubstantiated opinion that reflects an unduly restrictive view of these activities and their purpose. What the USPS-OIG recommends is inconsistent with the notion of proactive intelligence and law enforcement best practices.

**FINDING #1**

**Statement One**

Statement from USPS-OIG: Certain proactive intelligence searches that the Inspection Service conducted using an open-source intelligence tool exceeded the Postal Inspection Service's law enforcement authority because the search terms utilized by the Inspection Service did not have a postal nexus, and the agency is required to limit searches of that tool by only gathering information through searches that include postal terms.

Response: Disagree.

The Inspection Service was created to keep the American public, and the Postal Service safe, by enforcing more than 200 federal laws and investigating any crime that involves the mail.[1] The mission of the Inspection Service is to support and protect the Postal Service and its employees, infrastructure, and customers; enforce the laws that defend the nation's mail system from illegal or dangerous use; and ensure public trust in the mail. In particular, the Inspection Service is responsible for protection of the mails, enforcement of federal laws and postal regulations, plant and personnel security, and coordinating Postal Service emergency preparedness planning.[2] Postal Inspectors are granted police powers through federal statutes, authorizing them to conduct investigations into all allegations of postal law violations or misconduct, and make arrests in the enforcement of laws regarding the Postal Service or others laws of the United States if it's determined the violation of such laws will have a detrimental effect upon the operations of the Postal Service.[3] The Inspection Service also has incidental powers through the Postal Service which in general authorizes "all other powers incidental, necessary, or appropriate to the carrying on of its functions or the exercise of its specific powers."[4] In addition to these general powers, the Postal Service maintains specific powers, among others, "to investigate postal offenses and civil matters relating to the Postal Service."[5]

This authority has been addressed and expanded on in case law. The court in *U.S. v. Jones* stated, "Congress plainly intended the investigative authority conferred upon postal inspectors to extend to conduct that could reasonably be said to impair the proper operation of the Postal Service."[6] In a more recent case, the court issued a ruling with a similar sentiment echoing the *U.S. v. Jones* ruling by stating, "postal authority should not be limited by 'arbitrary criteria,' but rather courts should employ a 'flexible approach,' which considers the totality of the circumstances, when determining

[1] What Do United States Postal Inspectors Do? | USPIS
[2] Administrative Support Manual (ASM) 211.13
[3] 39 CFR § 233.1, 18 U.S.C. § 3061
[4] 39 U.S.C. § 401(10)
[5] 39 U.S.C. § 404(a)(6)
[6] *U.S. v. Jones*, 13 F.3d 100 (4th Cir. 1993)

how far authority extends under 3061 and 404(a)."[7] Another court stated this clearly by explaining "where…there exists a sufficient connection between the investigated conduct and postal operations or property, the statutory authority has not been exceeded."[8]

When considered collectively, these statutes and case law findings demonstrate that the Inspection Service has been given broad authority to investigate offenses related to the U.S. Mail; U.S. Postal Service employees, property, security, and operations; and customers of the Postal Service. These same legal authorities further grant the Inspection Service the ability and discretion to use a wide range of methods in furtherance of their mission. One such method used by the Inspection Service is open-source intelligence (OSINT).[9] OSINT is derived from the systematic collection, processing, and analysis of publicly available, relevant information in response to an investigative need.[10]

In their report, the USPS-OIG states a postal nexus is required in order for the Inspection Service to conduct open-source research, a basic position with which we agree. However, while it is beyond dispute that a postal nexus must exist to conduct this proactive research, the nexus must relate to the *purpose* of the search, and *not to the keywords being used to conduct the search as the USPS-OIG unreasonably posits*.

As evidenced in the statutes and case law above, and acknowledged by the USPS-OIG, the Inspection Service is responsible not only for investigating postal crimes but is also tasked with ensuring the safety and security of postal operations, people, and infrastructure. To meet this responsibility the Inspection Service must sometimes search for information which is not purely criminal in nature but may involve intelligence gathering on things such as a public health emergency or natural disaster. This directly implicates the agency's responsibility to the Postal Service and American people to assist in maintaining order, safeguarding postal employees and postal property, and ensuring continuity of postal operations. Given this, every search conducted by the Inspection Service, and reviewed by the USPS-OIG, had a postal nexus.

The USPS-OIG audit report's conclusion to the contrary is premised on the erroneous "form over substance" position that the key words the Inspection Service used to conduct open-source research had to have a postal nexus, instead of properly focusing on whether the search itself had a postal nexus. This myopic approach would quickly

---

[7] *Murray v. United States*, 2008 U.S. Dist. LEXIS 50054, 2008 WL 2622847

[8] *United States v. Lustig*, 865 F.2d 41 (2d Cir. 1989)

[9] Publicly available information is afforded very limited legal protections as is well established by case law. The Supreme Court provided guidance on this concept in *Katz v. United States* (389 U.S. 347, 351 (1967)) stating, "what a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[9] Other more recent cases such as *United States v. Warshak* ( 631 F.3d 266, 288 (6th Cir. 2010)) and *United States v. Jones* (132 S. Ct. 945 (2012)) discuss that same line of reasoning in their decisions and reaffirm the same general principal that information provided publicly constitutes an abandonment of privacy.

[10] https://irp.fas.org/doddir/army/atp2-22-9.pdf

lead to absurd results such as preventing the Inspection Service from looking at a parade route to ensure mail delivery in a certain location could safely continue without interruption. It would also deleteriously impact the Inspection Service's ability to determine whether any blue boxes on the parade route need to be removed from service or otherwise secured. Per the USPS-OIG recommendation, these would "exceed the Postal Inspection Service's law enforcement authority" since a postal term such as 'mail' or 'post office' was not included in the search. This reflects an overly formulaic approach to open-source research that is inconsistent with proactive intelligence gathering principles and law enforcement best practices. Attempting to comply with that narrow of a focus is unrealistic, not required by law or policy, and creates a real probability that relevant and necessary information would remain hidden.

As discussed above, using keywords that do not have a direct postal nexus will in many circumstances be critical to ensuring that searches return comprehensive results consistent with the underlying purpose. A recent example of these principles in practice, and where this type of research was successfully used, was during the summer of 2020 when widespread civil unrest took place across the country. Several of these incidents resulted in serious injury to people on site and extensive damage to vehicles and structures in the vicinity. One of the most serious incidents occurred in Minneapolis, Minnesota where two post offices were extensively damaged when they were set on fire and postal delivery vehicles were stolen. Another example of a significant event impacting postal employee safety and postal facility security was civil unrest in Chicago in the summer of 2020. Postal inspectors and local police had to conduct a rescue operation to evacuate postal employees from two post offices in an area experiencing civil unrest and looting.

In these instances, research was not used for the sole purpose of conducting an investigation. Instead, open-source intelligence was proactively reviewed with the intent of discovering information, actions, or activity that could impact the security of postal operations and the safety of postal employees in the area. The search terms were not unnecessarily restricted to those only having postal terms. Through these efforts, the Inspection Service was able to identify information such as the time, date, and locations where civil unrest were expected to take place in proximity to Postal Service people, property, and facilities, as well as to monitor real time updates of events while they were occurring that could impact postal operations. By reviewing this publicly available, widely shared, non-postal term content, the Inspection Service was able to prevent mail carriers from delivering mail on routes that would be unsafe, evacuate employees from postal facilities in areas experiencing unsafe conditions, and secure postal property such as facilities, vehicles, and blue collection boxes that could be damaged, or in turn be used to create more harm. In Minnesota and other places across the country, had the Inspection Service unreasonably limited its OSINT research to only use clearly identifiable postal terms (such as letter, post office, mail, etc.), it would have exponentially raised the risk of missing invaluable information needed to keep postal employees, facilities and property safe.

**Statement Two**

Statement from USPS-OIG: The Inspection Service is required to document the postal nexus within a request for assistance prior to it being submitted or to any work commencing.

Response: Disagree.

Section 2-210 of the Inspection Service's Case Management Reporting Guidelines states that cases are jacketed (opened) to document specific tasks in investigations conducted by the Inspection Service. When a new case is initiated and jacketed in the system, there is an approval process in place to ensure the case falls under Inspection Service purview and the entry was properly executed.[11] At the time of jacketing, the Postal Inspector states the nature of the investigation and explains the postal nexus.

As previously addressed, case law and statutes provide law enforcement agencies with broad discretion to conduct activities in furtherance of their mission. To initiate some of these types of activities, a Request for Assistance (RFA) is submitted by inspectors to support personnel such as analysts. Once an RFA is submitted into the task management system, a case number is required in order to proceed. The case number is a confirmation that a postal nexus exists since that is required when a case is opened in order for it to be approved and receive a corresponding case number.

In the report, USPS-OIG claims a requirement exists for specifically documenting the postal nexus in a submitted RFA, however no citation is offered to show where this requirement exists, and we are unable to find such a requirement. Further research on our part indicates USPS-OIG was unable to offer any basis for their opinion since there is no policy, procedure, statutory or legal basis requiring the postal nexus be documented within an RFA. The program operated in compliance with existing policy – a postal nexus is established to open a case and would be redundant to require in an RFA submission.

**Recommendation Responses**

**USPS-OIG Recommendation #1:** The Postal Inspection Service's Chief Counsel, in conjunction with the Postal Service Law Department, conduct a full review of the Analytics Team's responsibilities, activities, procedures, and any other associated guidance; and develop a process to ensure that all online analytical support activities conducted by the Postal Inspection Service are authorized.

Response: Agree. The Inspection Service agrees with this recommendation. This review will be completed within six months.

**USPS-OIG Recommendation #2:** The Inspector in Charge, Analytics, in consultation with the Postal Inspection Service's Chief Counsel, modify the Analytics Team's

[11] Inspection Service Case Management Reporting Guidelines, Section 230

Standard Operating Procedures to require the Office of Counsel to document its approval of all predefined keywords used for proactive intelligence searches, including approval for any changes to the predefined words.

Response: Agree in part. The Standard Operating Procedures will be updated to clarify that keywords utilized to conduct pre-defined automated search activities will require Office of Counsel review and approval prior to being established or changed. Proactive intel searches are different from these automated search activities, and it is premature to agree to any changes to this activity prior to the completion of the review agreed to in Recommendation #1.

**USPS-OIG Recommendation #3:** The Inspector in Charge, Analytics, in consultation with the Postal Inspection Service's Chief Counsel, modify the Analytics Team's Standard Operating Procedures to clarify documentation requirements for Requests for Assistance, to include requiring postal inspectors to document the postal nexus in their request.

Response: Disagree. Requests for Assistance are submitted under specific case numbers and those cases are opened based upon an existing Postal Nexus. It may be unnecessarily redundant for the information to be included in the request or to require an analyst second-guess the nexus determination already established at case opening. It is also premature to agree to this recommendation prior to the completion of review agreed to in Recommendation #1. If upon the completion of the review it is determined that adjustments to the Standard Operating Procedures are necessary, they will be made accordingly.

**USPS-OIG Recommendation #4:** The Inspector in Charge, Analytics, in consultation with the Postal Inspection Service's Chief Counsel, modify the Analytics Team's Standard Operating Procedures to require the Office of Counsel to document its approval of proactive work assignments at the time they are initiated.

Response: Disagree. Proactive work assignments have been and are conducted within the established policies, procedures, and legal authority of the Inspection Service. It is premature to agree to this recommendation prior to the completion of review agreed to in Recommendation #1. If upon the completion of the review it is determined that adjustments to the Standard Operating Procedures are necessary, they will be made accordingly.

**USPS-OIG Recommendation #5:** The Inspector in Charge, Analytics, in consultation with the Postal Inspection Service's Chief Counsel, modify the Analytics Team's Standard Operating Procedures to require that all reports identify the postal nexus.

Response: Disagree. Analysts conduct work within the scope and authority of the Inspection Service; therefore, it is not necessary to also identify the specific nexus in the report. Furthermore, it is premature to agree to this recommendation prior to the completion of review agreed to in Recommendation #1. If upon the completion of the

review it is determined that adjustments to the Standard Operating Procedures are necessary, they will be made accordingly.

**FINDING #2**

Statement from USPS-OIG: The Inspection Service did not properly maintain records associated with online analytical support activities.

Response: Disagree.

Analysis: When the Postal Service maintains, collects, uses, or disseminates information on individuals, that information must be covered by a System of Records (SOR). A SOR contains various types of information, the most pertinent to this finding being the retention and disposal of records.[12] The Postal Service may only collect personal information that is relevant or necessary to carry out an authorized purpose.[13] The Postal Service is prohibited from collecting or maintaining records describing or relating to how an individual exercises his or her rights under the First Amendment, except where the record is pertinent to and within the scope of an authorized law enforcement activity.[14]

The Inspection Service would maintain the records at issue here in SOR USPS 700.000, Inspection Service Investigative File System. One set of categories of individuals in the system is for subjects of investigations, complainants, informants, witnesses, and other individuals in investigations. The purpose of the SOR is, in part, to support investigations of criminal, civil, or administrative matters.

As already discussed in the response to Finding #1, the Inspection Service was conducting authorized law enforcement activity when it conducted its searches. This includes the proactive efforts by analysts. Where there was information discovered, it was retained pursuant to the SOR. Where information no longer had value or had no law enforcement purpose for being kept it was discarded. By not retaining information, the Inspection Service adhered to the prohibition on purposeless retention of potentially First Amendment related activity.

The USPS-OIG acknowledges these efforts at protecting the privacy interests of the American public in its finding. Specifically, the USPS-OIG noted some information reviewed would contain PII information and that the information was not kept if it was not needed in a final report. The USPS-OIG thereafter unreasonably concludes that the analyst's efforts at adhering to the policy set forth in AS-353 to prohibit the unnecessary retention of potential First Amendment related information is problematic.

---

[12] AS-353, Section 3-2.1.
[13] AS-353, Section 3-3.1.
[14] AS-353, Section 3-3.3.

The USPS-OIG finding would seem to require the Inspection Service to retain a broad-based surveillance apparatus containing sensitive data on individuals even when that data no longer has a legitimate law enforcement purpose. The Inspection Service cannot agree to this requirement.

For all the reasons stated above, the Inspection Service has properly maintained records associated with online analytical support activities.

**Recommendation Response**

**USPS-OIG Recommendation #6:** The Inspector in Charge, Analytics, develop procedures for retaining documentation associated with work completed by the Analytics Team and storing sensitive information to ensure compliance with Postal Service Policy.

Response: Agree in part. We comply with the current Postal Service policies regarding the storage of sensitive information. Subsequent to the review conducted as part of Recommendation # 1, procedures will be adjusted if it is determined to be appropriate to do so regarding the retention of information.

**FINDING #3**

Statement from USPS-OIG: The Inspection Service's Contracting Officer Representative (COR) did not prepare letters of appointment in a timely manner for two of the seven contracts awarded for products and services used by iCOP.

Response: Agree. This finding has already been rectified by U.S. Postal Service-Supply Management.

In regard to Table 2, *Contracts Awarded for iCOP*, the USPS-OIG inaccurately attributed all the costs associated to these tools directly to the iCOP program. While the program did utilize some of those tools, the majority of the usage was done by the agency as a whole. Out of the $11.9 million dollars in total contracts, $5.7 million is directly attributable to the iCOP Program, with $4.7 million associated with contracts for personnel. Of that total amount, over 97% of the work performed by the iCOP Program was in direct support of ongoing criminal investigations, and less than 3% related to the general research and review of open source information.

Most disappointingly, the USPS-OIG failed to acknowledge any of the benefits that the iCOP program has provided to the agency. The program has supported numerous investigations which has successfully resulted in the arrest of more than 300 individuals and the tracking and analysis of over $660 million dollars in cryptocurrency.

**CONCLUSION**

The analysis offered herein demonstrates that the Inspection Service did not exceed its authority and appropriately conducted open-source research based on that authority and a clear postal nexus. In addition, this response also demonstrates that the Inspection Service does in fact properly maintain records associated with online analytical support activities and provides sound legal reasoning for that assertion. This response provides data and statistics to clarify the contracts and costs of law enforcement tools used by the Inspection Service. Finally, this response fairly addresses all the recommendations made in the USPS-OIG report and offers demonstrated action items to justify those responses. Overall, the Inspection Service is confident that the analysis and explanations provided herein will offer an accurate, and more complete understanding of the programs and methods used by the Inspection Service in its unwavering dedication to protect and support the U.S. Postal Service and the American people.

Sincerely,

E-SIGNED by Gary.R Barksdale
on 2022-03-17 12:29:28 CDT

Gary R. Barksdale
Chief Postal Inspector

E-SIGNED by Thomas.J Marshall
on 2022-03-17 09:25:44 CDT

Thomas J. Marshall
General Counsel and Executive Vice President

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